Diplomarbeit

Zur Erlangung des akademischen Grades
eines Magisters der Rechtswissenschaften

an der Karl-Franzens-Universität Graz.

„Hacktivismus“ – Die Macht sozialer Netzwerke. Eine (computer-)strafrechtliche Betrachtung.

Vorgelegt von
Martin SCHOPPER

Beurteiler: Assoz. Prof. Mag. Dr. iur. Christian BERGAUER
am Institut für Rechtsphilosophie, Rechtssoziologie und Rechtsinformatik

Graz, 2015

Ehrenwörtliche Erklärung

Ich erkläre ehrenwörtlich, dass ich die vorliegende Arbeit selbständig und ohne fremde Hilfe verfasst, andere als die angegebenen Quellen nicht benutzt und die den Quellen wörtlich oder inhaltlich entnommenen Stellen als solche kenntlich gemacht habe. Die Arbeit wurde bisher in gleicher oder ähnlicher Form keiner anderen inländischen oder ausländischen Prüfungsbehörde vorgelegt und auch noch nicht veröffentlicht. Die vorliegende Fassung entspricht der eingereichten elektronischen Version.

Datum Unterschrift

Inhaltsverzeichnis

Abkürzungsverzeichnis

aA	andere Ansicht
ABl	Amtsblatt
Abs	Absatz
aF	alte Fassung
Art	Artikel
AT	Allgemeiner Teil
BGBl	Bundesgesetzblatt
BlgNR	Beilagen zu den Stenographischen Protokollen des Nationalrats
BMJ	Bundesministerium für Justiz
bspw	beispielsweise
BT	Besonderer Teil
bzw	beziehungsweise
ca	circa
CyCC	Cyber-Crime-Convention
DDoS	Distributed Denial of Service
dh	das heißt
DoS	Denial of Service
DSG	Datenschutzgesetz
ErlRV	Erläuternde Bemerkungen zur Regierungsvorlage
ErwG	Erwägungsgrund
EU	Europäische Union
f, ff	und der/die folgende(n)
gem	gemäß
hL	herrschende Lehre
hM	herrschende Meinung
Hrsg	Herausgeber
idF	in der Fassung
idR	in der Regel
IKT	Informations- und Kommunikationstechnologie
insb	insbesondere
iSd	im Sinne des
ISO	International Organization for Standardization
iSv	im Sinne von
IT	Informationstechnologie
IuK	Informations- und Kommunikations(-tools)

iVm	in Verbindung mit
iwS	im weiteren Sinn
JAB	Justizausschussbericht
leg cit	legis citatae
lit	Litera
mE	meines Erachtens
OSI	Open Systems Interconnection
PIPA	Protect IP Act
RB	Rahmenbeschluss
RL	Richtlinie
Rsp	Rechtsprechung
RV	Regierungsvorlage
Rz	Randzahl
SbgK	Salzburger Kommentar zum Strafgesetzbuch
sog	sogenannte/er/es
SOPA	Stop Online Privacy Act
StGB	Strafgesetzbuch
StRÄG	Strafrechtsänderungsgesetz
TKG	Telekommunikationsgesetz
ua	unter anderem
udgl	und dergleichen
usw	und so weiter
uU	unter Umständen
vgl	vergleiche
WK	Wiener Kommentar zum Strafgesetzbuch
Z	Ziffer
zB	zum Beispiel
ZuKG	Zugangskontrollgesetz
zust	zustimmend

1. Einführung

Die weltweite Vernetzung von Computersystemen hat sämtliche Lebens-, Gesellschafts- und Wirtschaftsbereiche nachhaltig verändert. Internet-Suchmaschinen dienen der raschen Auffindung bereitgestellter Informationen im Cyberspace. Virtuelle Flohmärkte erleichtern den Kauf und Verkauf gebrauchter Sachen. Facebook, Twitter und Co sind beliebte Treffpunkte für Millionen Internetnutzer. Der Elektronische Rechtsverkehr ermöglicht die digitale Kommunikation zwischen Verfahrensbeteiligten und Gerichten bzw Staatsanwaltschaften.[1] Die Einsatzmöglichkeiten des Internet sind nahezu grenzenlos und aus unserer modernen Gesellschaft kaum mehr wegzudenken.

Dieser technische Fortschritt sowie die zunehmende Vernetzung schaffen jedoch neue Kriminalitätsformen und Phänomene.[2] Organisierte und arbeitsteilig agierende Gruppen von Kriminellen verwenden modernste Technik und verlegen die Tatorte in die virtuelle Welt des Cyberspace. Die Angriffsziele sind vielfältig und bedrohen Computersysteme von Institutionen, Behörden sowie Unternehmen.[3] Als Hauptmotivationen im Bereich der Cyber-Kriminalität sind einerseits finanzielle Interessen, Geltungsdrang oder Langeweile anzuführen. Andererseits können Angriffe auf Computersysteme und Daten politisch motiviert stattfinden und werden unter dem schillernden Begriff „Hacktivismus“ zusammengefasst.[4]

Die vorliegende Arbeit beschäftigt sich zunächst mit Grundlagen und Begriffen aus dem Bereich der Computer-, Netzwerk-, und Internettechnik. Zudem werden die häufigsten Bedrohungen und Gefahren im Cyberspace aufgezeigt. Kapitel 3 und 4 beleuchtet das Phänomen „Hacktivismus“ und die damit in Verbindung stehenden Akteure.

Im Hauptkapitel der vorliegenden Arbeit „Computerstrafrechtliche Betrachtung“ werden die kernstrafrechtlichen Computerdelikte (§§ 118a, 126a, 126b und 126c StGB[5]) im Allgemeinen dargestellt. Die auf derartige Sachverhalte allenfalls anwendbaren „klassischen“ Delikte des Kriminalstrafrechts, wie etwa die Nötigung (§ 105), Sachbeschädigung (§ 125) oder Erpressung (§ 144) werden im Rahmen dieser Arbeit außer Betracht gelassen. Die internationalen Aspekte des Strafrechts finden ebenfalls keine Berücksichtigung.

---

1 <digitales.oesterreich.gv.at/site/6351/default.aspx> (25.4.2015).
2 *Reindl-Krauskopf*, Cyberstrafrecht im Wandel, ÖJZ 2015/19, 112 (112).
3 *Bundeskriminalamt*, Cybercrime in Österreich: Report 2013, 4 <bmi.gv.at/cms/BK/presse/files/Cybercrime_Report_2013.pdf> (26.10.2014).
4 <teltarif.de/hacker-angriff-2011-rueckblick-ausblick-2012/news/44946.html> (23.9.2014).
5 Bundesgesetz vom 23. Jänner 1974 über die mit gerichtlicher Strafe bedrohten Handlungen (Strafgesetzbuch – StGB), BGBl 60/1974 idF I 106/2014; Rechtsnormen ohne Quellenangabe beziehen sich auf das StGB.

Im Anschluss an die allgemeine Darstellung der zu untersuchenden Computerstrafdelikte erfolgt eine Analyse, ob bzw inwieweit diese auf ausgewählte „hacktivistische“ Erscheinungsformen anwendbar sind. Da zur Zeit der Fertigstellung dieser Arbeit die im Juni 2015 im Parlament eingelangte Regierungsvorlage zum StRÄG 2015[6] vom Nationalrat mittlerweile beschlossen wurde, werden die geplanten Änderungen der Computerdelikte (§§ 118a, 126a und 126b) im Überblick vorgestellt.

[6] RV 689 BlgNR XXV. GP (StRÄG 2015).

2. Technische Grundlagen und Begriffe

2.1. Computer-, Netzwerk- und Internettechnik

Digitalcomputer (zB PCs[7]) sind programmgesteuerte Rechenmaschinen, die auf elektronischer Basis Daten verarbeiten.[8] Die physischen Bauteile eines Rechners (zB Prozessor[9], Arbeitsspeicher[10]) sowie anschließbare Peripheriegeräte (Bildschirm, Tastatur, Drucker udgl) werden als Hardware bezeichnet.[11] Computer wären ohne den Einsatz entsprechender Software (zB Betriebssystem, Gerätetreiber[12], Textverarbeitungsprogramme) nutzlos.[13]

Das „EVA-Prinzip" beschreibt das Grundprinzip der elektronischen Datenverarbeitung und somit die Funktionsweise eines Rechners (Eingabe – Verarbeitung – Ausgabe).[14] Unter Daten versteht man Fakten bzw Informationselemente (zB Ziffern, Buchstaben, Klänge), die ein Rechner auf der Grundlage des binären Zahlensystems, bestehend aus Nullen und Einsen, nach einem festgelegten Schema (Computerprogramm) verarbeitet.[15] Die kleinste Darstellungseinheit wird als Bit[16] (0 oder 1) bezeichnet. Dateien sind organisatorisch zusammenhängende Datenmengen (zB Computerprogramme, Bilder oder Textdokumente), die auf einem Datenträger gespeichert werden.[17] Datenbanken, bestehend aus Tabellen und Datensätzen, dienen der strukturierten Speicherung und Verwaltung digitaler Daten.[18] Die Erstellung und Bearbeitung von Datensätzen bzw Datenbanken erfolgt weitgehend mit der Befehlssprache SQL[19].

Computer werden heutzutage allerdings kaum mehr als „stand-alone-PCs" verwendet, sondern in lokalen Rechnernetzen (zB Firmen- oder Heim-Netzwerke) verbunden oder

---

7 Personal Computer sind universell einsetzbare Rechner, die je nach Bauart unterschiedlich bezeichnet werden (zB Desktop-PC, Laptop, Notebook, Tablet-PC); <itwissen.info/definition/lexikon/Personal-Computer-PC-personal-computer.html> (10.9.2014).

8 <itwissen.info/definition/lexikon/Computer-computer.html> (10.9.2014).

9 Der Prozessor ist ein Mikrochip, bestehend aus Rechen- und Steuerwerk, der Befehle verarbeitet und als Taktgeber fungiert; vgl dazu *Ortmann*, PC-Grundlagen[8] (2003) 30 f.

10 Im Arbeitsspeicher werden Daten kurzfristig abgelegt, die ein Rechner zur Verarbeitung benötigt; *Ortmann*, PC-Grundlagen[8], 31 f.

11 *Gumm/Sommer*, Einführung in die Informatik[10] (2012) 35 ff.

12 Treiber sind Programme zur Ansteuerung von Software- oder Hardware-Komponenten; vgl *Gumm/Sommer*, Einführung in die Informatik[10], 61.

13 *Gumm/Sommer*, Einführung in die Informatik[10], 58 ff.

14 Vgl *Ernst/Schmidt/Beneken*, Grundkurs Informatik: Grundlagen und Konzepte für die erfolgreiche IT-Praxis[5] (2015) 12.

15 *Badertscher/Gubelmann/Scheuring*, Wirtschaftsinformatik Grundlagen: Informations- und Kommunikationssysteme gestalten (2006) 31 ff.

16 Abkürzung für Binary Digit.

17 *Gumm/Sommer*, Einführung in die Informatik[10], 8; *Badertscher/Gubelmann/Scheuring*, Wirtschaftsinformatik Grundlagen, 41 f.

18 *Badertscher/Gubelmann/Scheuring*, Wirtschaftsinformatik Grundlagen, 42 ff.

19 Abkürzung für Structured Query Language.

verfügen über separate Internetanbindungen. Computernetzwerke werden je nach Anordnung der Netzwerkrechner (Netzwerktopologie),[20] der Art ihrer Verbindung,[21] aufgrund der räumlichen Ausdehnung[22] oder der Anwendungsverteilung in Klassen eingeteilt.[23] Im Bereich der Anwendungsverteilung sind insb Peer-to-Peer- (kurz P2P) von Client-Server-Netzen zu unterscheiden.[24] Erstere bezeichnen den Zusammenschluss gleichberechtigter Rechner, die sowohl Ressourcen anderer Computer in Anspruch nehmen als auch eigene zur Verfügung stellen. In Client-Server-Netzen bieten ausschließlich Server[25] unterschiedliche Dienste an (zB Web-Server, Datenbank-Server). Clients[26] treten demgegenüber als reine Dienstnehmer auf. Terminal- bzw Mainframe-Architekturen zählen seit der Markteinführung der PCs zu den antiquierten Erscheinungsformen.[27]

Das Internet ist das weltweit größte Netzwerk, bestehend aus einer Vielzahl einzelner Computernetze, die durch Netzknoten (zB Router[28]) verbunden sind.[29] Der Datenaustausch erfolgt auf der Grundlage standardisierter Normen, die als Netzwerk- bzw Internet-Protokolle bezeichnet werden.[30] Deren Aufgaben und Funktionsweisen werden in den „RFCs“[31] erläutert. Je nach Aufgabenverteilung lassen sich Internet-Protokolle einer der 7 Schichten des ISO/OSI-Referenzmodells[32] zuordnen.[33] Die unterste Schicht dieses Modells (Bitübertragungsschicht) regelt die Ausgestaltung physikalischer Komponenten (zB Netzwerkkarten, Kabeltypen, oder drahtlose Übertragungsgeräte) und ermöglicht somit die Übertragung von Signalen (sog „Daten- oder Bitströme“).[34] Die transportorientierten Protokolle der darüber liegenden Schichten 2 bis 4 (Sicherungs-, Vermittlungs- und Transportschicht)

---

20 Im Bereich der lokalen Netze wird grob zwischen Bus-, Stern-, Ring- und Baum-Netzen unterschieden.

21 Computernetze werden je nach Art der Verbindung in drahtgebundene oder drahtlose Netze eingeteilt; siehe dazu *Badertscher/Gubelmann/Scheuring,* Wirtschaftsinformatik Grundlagen, 57.

22 Aufgrund der unterschiedlichen räumlichen Ausdehnung eines Netzes wird bspw zwischen Local Area Network (LAN) und Wide Area Network (WAN) abgegrenzt; vgl *Kammermann*, CompTIA Network+[5] (2012) 30 f.

23 Ausführlich dazu *Scherff*, Grundkurs Computernetzwerke: Eine praktische Einführung in Netzwerk- und Internet-Technologien[2] (2010) 8 ff.

24 *Scherff*, Grundkurs Computernetzwerke[2], 12.

25 Der Begriff Server ist mehrdeutig und bezeichnet sowohl Software als auch Hardware; vgl dazu *Badertscher/Gubelmann/Scheuring*, Wirtschaftsinformatik Grundlagen, 25.

26 Die Bezeichnung Client umfasst Software oder Hardware.

27 *Badertscher/Gubelmann/Scheuring*, Wirtschaftsinformatik Grundlagen, 22.

28 Als Router werden konfigurierte Netzwerkrechner bezeichnet, die auf der Grundlage von Routingtabellen oder eigenen Protokollen die Datenübertragung übernehmen; vgl *Kammermann*, CompTIA Network+[5], 89 f.

29 *Gumm/Sommer*, Einführung in die Informatik[10], 635 ff.

30 *Badertscher/Gubelmann/Scheuring*, Wirtschaftsinformatik Grundlagen, 61.

31 Request for Comments sind Dokumente, die technische Erläuterungen und Verbesserungsvorschläge zu Netzwerk- bzw Internet-Protokollen enthalten; vgl dazu <rfc-editor.org/> (16.9.2014).

32 Das OSI-Modell wurde von der ISO entwickelt, um die Kommunikation zwischen verschiedenen Computersystemen einzelner Hersteller, sowie die autonome Weiterentwicklung der Technologien innerhalb einer Schicht zu ermöglichen.

33 *Eckert*, IT-Sicherheit: Konzepte – Verfahren – Protokolle[6] (2009) 87 ff; vgl auch *Kammermann,* CompTIA Network+[5], 33 ff.

34 *Kammermann*, CompTIA Network+[5], 38.

gewährleisten insb die fehlerfreie Datenübertragung (ICMP[35]), den Versand der Daten vom Sender zum Empfänger (IP[36]), sowie das Fragmentieren der zu übermittelnden Daten in Pakete (TCP[37]). Die Protokolle der anwendungsorientierten Schichten 5 bis 7 (Sitzungs-, Darstellungs- und Anwendungsschicht) übernehmen Aufgaben wie etwa das Ver- und Entschlüsseln von Daten (zB TLS[38]) oder stellen unterschiedliche Funktionen (SMTP[39], HTTP[40]) für Internetdienste wie etwa Web, E-Mail oder Chat bereit. IP-Adressen dienen der Identifikation einzelner Rechner im Internet, die dadurch für andere Kommunikationspartner erreichbar werden.[41] IPv4-Adressen bestehen aus 4 Segmenten, die Zahlenwerte zwischen 0 und 255 annehmen können und durch Punkte voneinander getrennt sind (zB 192.0.2.42).[42] Die Zuweisung von IP-Adressen an Rechner (zB Router, Web-Server) kann statisch oder dynamisch (zB durch DHCP-Server[43]) erfolgen. Zur Identifizierung einzelner Dienste reicht die IP-Adresse allerdings dann nicht aus, wenn mehrere Services auf einem Host[44] verfügbar sind. Daher werden zusätzlich Portnummern verwendet.[45] Diese Nummern sind den Standarddiensten im Internet (zB Port 80 für Web-Server, Port 25 für SMTP-Server) fest zugewiesen.[46] Ports und IP-Adressen bilden gemeinsam sog „Sockets“, die einerseits die Kommunikation zwischen 2 bestimmten Teilnehmern sichern und andererseits die gleichzeitige Verbindung mehrerer Clients zum Server zulassen.[47] Eine bedeutende Funktion im Internet übernimmt darüber hinaus das sog „Domain-Name-System“ (kurz DNS). Im konkreten Zusammenhang haben Name-Server als Bestandteil eines weltweit verfügbaren Systems von Datenbanken die Aufgabe, Domain-Namen (zB uni-graz.at) in IP-Adressen und umgekehrt zu übersetzen.[48] HTML-Dokumente[49], bestehend aus Texten, Grafiken, Hyperlinks oder anderen Inhalten, werden als Webseiten bezeichnet, die durch Eingabe des URL[50] im

---

35 Siehe dazu RFC 792 <rfc-editor.org/rfc/rfc792.txt> (16.9.2014).

36 Siehe RFC 791 <rfc-editor.org/rfc/rfc791.txt> (16.9.2014).

37 Das Transmission Control Protocol ist im Vergleich zum User Datagram Protocol (kurz UDP) ein verbindungsorientiertes Protokoll; siehe RFC 793 <rfc-editor.org/rfc/rfc793.txt> (16.9.2014); vgl dazu auch *Kammermann*, CompTIA Network+[5], 205; *Gumm/Sommer*, Einführung in die Informatik[10], 320 f.

38 Das Netzwerk- und Internetprotokoll Transport Layer Security wird etwa zur Verschlüsselung von E-Mails eingesetzt; vgl dazu RFC 3207 < rfc-editor.org/rfc/rfc3207.txt> (18.9.2014).

39 Das Simple Mail Transfer Protocol übernimmt das Versenden und Weiterleiten von E-Mails; vgl RFC 5336 <rfc-editor.org/rfc/rfc5336.txt> (18.9.2014).

40 Mithilfe des Hypertext Transfer Protocols werden Webseiten in den Browser geladen; vgl RFC 7230 <rfc-editor.org/rfc/rfc7230.txt> (18.9.2014).

41 *Gumm/Sommer*, Einführung in die Informatik[10], 643 ff.

42 Vgl RFC 791.

43 Das Kommunikationsprotokoll DHCP dient der dynamischen bzw automatischen Zuweisung von IP-Adressen an Clients; vgl RFC 2131 <rfc-editor.org/rfc/rfc2131.txt> (18.9.2014).

44 Als Host wird ein Netzwerkrechner bezeichnet, der Dienste für andere Computer zur Verfügung stellt.

45 *Jarzyna*, TCP/IP: Grundlagen, Adressierung, Subnetting (2013) 69 ff.

46 *Blumhagel/Joos*, Netzwerke: geheime Tricks – perfekt vernetzt! (2005) 207; vgl dazu auch *Kammermann*, CompTIA Network+[5], 206.

47 *Blumhagel/Joos*, Netzwerke, 206 f.

48 *Eckert*, IT-Sicherheit[6], 120 ff.

49 Die Auszeichnungssprache Hypertext Markup Language dient der Strukturierung und Gestaltung von Webseiten und wird meist in Kombination mit Cascading Stile Sheets (kurz CSS) eingesetzt.

50 Abkürzung für Uniform Ressource Locator (zB http://www.uni-graz.at).

Browser aufrufbar sind.[51] Die Erstellung und Verwaltung einer Website[52] erfolgt üblicherweise durch den Einsatz sog „Web-CMS“[53], die zumeist direkt am Web-Server platziert sind. Der Zugang zu solchen Programmen ist idR passwortgeschützt, um unberechtigte Veränderungen der Seiteninhalte zu verhindern. Im Unterschied zu statischen Webseiten, die als Dateien auf einem Web-Server abgelegt sind und durch diesen an den Browser übergeben werden, erfolgt die Erzeugung der Inhalte dynamischer Seiten (zB Online-Shop, Gästebuch) direkt zum Zeitpunkt des Aufrufs.[54] Soziale Netzwerke im Internet (auch Web-Plattformen, Portale, oder Social-Media-Communities genannt) sind aus technischer Sicht dynamische Webseiten, die für User unterschiedliche Funktionen und Anwendungen (bspw Chat, Suchfunktionen, Bild-Video- oder Textverarbeitungssoftware) bereitstellen, um eigene Inhalte zu erzeugen.[55] Die Funktionsweise sozialer Netzwerke ist idR ähnlich. Nach der Registrierung mit dem wahren Namen oder einem Nicknamen[56], der Mail-Adresse und einem Passwort können NutzerInnen individuelle Profile, dh eine eigene Webseite mit persönlichen Angaben (zB Geburtsdatum, Wohnadresse, Beruf) erstellen und dadurch mit anderen TeilnehmerInnen in Kontakt treten. Bekannte soziale Netzwerke sind Facebook[57], der Micro-Blogging-Dienst Twitter[58] und das beliebte Video-Portal YouTube[59].

2.2. Bedrohungen und Gefahren im Internet

2.2.1. Hacking: Ablauf einer Attacke

Die Tätigkeit eines Hackers wird „Hacking“ oder „Hacken“ bezeichnet.[60] Das Ergebnis ist ein „Hack“ und bezieht sich im Bereich der Computersicherheit insb auf die Erforschung und Ausnutzung von Schwachstellen in Computerprogrammen.[61] Böswillige Hacking-Angriffe sowie Penetration-Tests[62] erfolgen grundsätzlich in 5 Schritten.[63]

---

51 *Jendryschik,* Einführung in XHTML, CSS und Webdesign: Standardkonforme, moderne und barrierefreie Websites erstellen[2] (2009) 25 ff.

52 Der Begriff Website bezeichnet den gesamten Web-Auftritt (dh eine Site besteht aus mehreren Dokumenten, die miteinander verlinkt sind).

53 Als Content-Management-Systeme werden Tools bezeichnet, die der Verwaltung von Inhalten dienen; vgl dazu <itwissen.info/definition/lexikon/content-management-system-CMS-Content-Managementsystem.html> (19.9.2014).

54 *Jendryschik*, Einführung in XHTML, CSS und Webdesign[2], 26.

55 <itwissen.info/definition/lexikon/Soziales-Netzwerk-social-network.html> (19.9.2014).

56 Nicknamen sind selbst gewählte Fantasienamen, unter denen jemand im Internet (zB Chat) auftritt; vgl <duden.de/rechtschreibung/Nickname> (4.10.2014).

57 <facebook.com> (4.10.2014).

58 <twitter.com> (4.10.2014).

59 <youtube.com> (4.10.2014).

60 <de.wikipedia.org/wiki/Hacker> (3.10.2014).

61 <de.wikipedia.org/wiki/Hacker_(Computersicherheit)> (3.10.2014).

62 Durch diese zustimmungsbedürftigen Tests simulieren IT-Sicherheitsunternehmen Angriffe auf Computer und Netzwerke, um diese auf Angriffspunkte zu überprüfen; <sicherheitskultur.at/Pen_tests.htm> (4.10.2014).

63 Siehe *NetSecure-IT*, Whitepaper „Hackerdefinition“: Hacker (Motive) und Angriffstechniken, 14 <whitepaper.netsecure-it.de/Hackerdefinition.pdf> (4.10.2014); <blog.emagined.com/2009/05/08/the-five-phase-approach-of-malicious-hackers/> (4.10.2014).

In der ersten Phase sammeln Angreifer durch den Einsatz von Internet-Suchmaschinen (Google, Bing), Online-Datenbanken (zB Whois[64]), aber auch mithilfe alternativer Methoden (Social-Engineering) frei verfügbare Informationen über das Zielsystem (zB IP-Adressen, Passwörter).[65] Im nächsten Schritt, der sog „Scanning-Phase", werden Port- bzw Schwachstellenscanner (zB Nmap[66] oder Nessus[67]) verwendet, um festzustellen, welche Dienste auf dem Rechner aktiv sind und welche Schwachstellen etwa das Betriebssystem aufweist.[68] In der Angriffsphase verwerten Hacker die erlangten Informationen und verschaffen sich Zugang zum System, indem idR Sicherheitslücken in Computerprogrammen ausnutzt werden.[69] Nach erfolgreicher Durchführung der Attacke ist es darüber hinaus auch das Ziel, den Zugriff auf das fremde System so lange wie möglich aufrecht zu erhalten. Daher wird ein Hacker zumeist versuchen, Administratorenrechte (auch Root-Rechte[70] genannt) zu erlangen. Im konkreten Zusammenhang sind insb Rootkits[71] in Verwendung, um Aktivitäten auf dem angegriffenen Rechner zu verschleiern.[72]

2.2.2. Web-Hacking-Techniken im Überblick

Web-Hacking bezeichnet eine Teildisziplin des Hacking und erfasst im Speziellen Angriffe auf Web-Anwendungen und Webseiten. Diese Hacking-Methoden stützen sich im Wesentlichen auf Programmierfehler bei der Entwicklung von Webseiten.[73]

2.2.2.1. Brute-Force-Methode

Brute-Force ist eine in der Praxis häufig verwendete Technik zum systematischen Herausfinden von Passwörtern, um sich Zugang zu fremden Benutzerkonten zu verschaffen.[74] Im Rahmen solcher Attacken werden idR automatisierte Tools (zB John the Ripper[75]) eingesetzt, die sämtliche Kombinationen eines Zugangsschlüssels mit „roher Gewalt" durchprobieren.[76] Im Zuge eines Brute-Force-Angriffs sind bspw Passwortlisten in Verwendung, die häufig vorkommende Geheimwörter enthalten (Wörterbuch-Attacken).[77]

---

64 Siehe dazu die Webseite <who.is> (19.10.2014).
65 *Winterer*, Windows 7 Sicherheit (2011) 56.
66 <nmap.org/download.html> (19.10.2014).
67 <sectools.org/tool/nessus/> (19.10.2014).
68 *Kappes*, Netzwerk- und Datensicherheit: Eine praktische Einführung[2] (2013) 238 ff.
69 *Winterer*, Windows 7 Sicherheit, 57.
70 Root-Rechte sind weitreichende und umfassende Zugriffsrechte.
71 Diese Schadprogramme erlauben dem Angreifer die unentdeckte Installation weiterer Programme auf dem infizierten Rechner; vgl <blog.kaspersky.de/was-ist-ein-rootkit/853/> (19.10.2014).
72 *Eckert*, IT-Sicherheit[6], 27.
73 Vgl dazu *Ziegler*, Web Hacking: Sicherheitslücken in Webanwendungen - Lösungswege für Entwickler (2014) Vorwort XII f.
74 *Ziegler*, Web Hacking, 15 ff.
75 <sectools.org/tool/john/> (20.10.2014).
76 *Winterer*, Windows 7 Sicherheit, 61 ff.
77 *Ziegler*, Web Hacking, 22.

Unter einer „Reverse-Brute-Force-Attacke“ ist eine Angriffsmethode zu verstehen, bei der bestimmte Zugriffscodes an mehreren Benutzerkonten zugleich getestet werden.[78] Im Zusammenhang mit verschlüsselten Kennwörtern ist anzumerken, dass der verwendete Verschlüsselungsalgorithmus mithilfe sog „Rainbow-Tables“[79] herausgefunden werden kann.[80] Der zeitliche Aufwand, ein Passwort zu „knacken“, hängt letztendlich von mehreren Faktoren ab (zB Länge der Wörter, Klartextnamen, verschlüsselte Zugriffscodes, Verteilung auf mehrere Rechner).[81] Im Unterschied zu anderen Web-Hacking-Techniken nutzt diese Methode keine durch Programmierfehler verursachten Schwachstellen in Anwendungen, sondern „schwache“ Passwörter aus.[82]

2.2.2.2. SQL-Injection

Dynamische Webseiten (zB Online-Shops) sind idR mit Datenbanken verbunden, die der Speicherung von Kundendaten (Name, Geburtsdatum, oder Kreditkartennummern udgl) dienen. SQL-Injection bedeutet, dass Programmierfehler, im konkreten Fall die mangelnde Überprüfung der Dateneingabe in Online-Formularen, ausgenutzt werden, um SQL-Befehle in Datenbanken einzuschleusen.[83] Angreifer sind dadurch in der Lage, einzelne Datensätze oder Tabellen mittels „UPDATE“-Befehl zu ändern (zB Grafiken oder Texte einer Webseite), mithilfe der Befehle „DELETE“ bzw „DROP“ zu löschen oder durch die Eingabe des „INSERT“-Befehls Daten hinzuzufügen. Um SQL-Code einzuschleusen, werden idR bestehende Verbindungen zwischen Zielseite, Web- und Datenbank-Server ausgenutzt.[84]

2.2.2.3. Cross-Site-Scripting

Im Rahmen von Cross-Site-Scripting-Attacken (kurz XSS) wird versucht, HTML-Code oder ein Skript[85] in Webseiten einzubinden.[86] Das Angriffsziel dieser Methode ist idR nicht die Webseite, sondern der Besucher einer Seite. Bei reflektierten und persistenten XSS-Attacken wird injizierter Code vom Server ungeprüft an den Client des Opfers übergeben.[87] Im Gegensatz dazu wird clientseitiges XSS eingesetzt, um HTML- oder JavaScript-Code[88] in statische Webseiten einzuschleusen. Diese Methode ermöglicht etwa die Unterbringung von

78 *Ziegler*, Web Hacking, 25.
79 Rainbow-Tables sind Tabellen, die zur Bestimmung des Klartextnamens eingesetzt werden.
80 *Ziegler*, Web Hacking, 26 ff.
81 *Ziegler*, Web Hacking, 29 ff.
82 *Ziegler*, Web Hacking, 7.
83 <heise.de/security/artikel/Giftspritze-270382.html> (13.10.2014); ausführlich dazu *Ziegler*, Web Hacking, 75 ff.
84 *Ziegler*, Web Hacking, 79.
85 Als Skript wird ein kleineres Programm bezeichnet, das in einer Skriptsprache geschrieben ist (zB PHP, JavaScript).
86 *Ziegler*, Web Hacking, 89 f.
87 *Ziegler*, Web Hacking, 90 ff.
88 Java Script ist eine Programmiersprache, die zur Entwicklung von Web-Anwendungen eingesetzt wird.

Schadprogrammen (zB Trojaner) auf vertrauenswürdigen Webseiten, um damit fremde Rechner zu infizieren (sog „Drive-by-Downloads“).[89] Cross-Site-Tracing ist eine besonders gefährliche XSS-Variante.[90] Dadurch kann eine bestehende Verbindung zwischen Kommunikationspartnern „entführt“ werden, um etwa Zugangsdaten zu erlangen („Session-Hijacking“).

2.2.2.4. Buffer-Overflow

Überläufe des Arbeitsspeichers, auch Buffer-Overflows genannt, sind häufig vorkommende Schwachstellen in Programmen.[91] Dabei wird die Eingabe zu langer Zeichenketten für zu klein reservierte Speicherbereiche ungeprüft zugelassen und ermöglicht das Überschreiben der Inhalte des Arbeitsspeichers, um etwa Computerprogramme zum Absturz zu bringen.[92] Im konkreten Zusammenhang besteht auch die Gefahr, dass Angreifer eigenen Befehlscode gezielt einschleusen, um bspw Authentifizierungen zu umgehen.[93] Dadurch erhalten sie im besten Fall den Systemzugriff mit den Rechten eines Administrators.

2.2.2.5. Buffer Over-Read

Der „Heartbleed-Exploit“ ermöglichte das Auslesen von Daten aus dem Arbeitsspeicher eines Rechners.[94] Angreifer nutzten eine zunächst unerkannte Schwachstelle (Zero-Day-Exploit) der Heartbeat-Erweiterung des Verschlüsselungsprotokolls TLS in der freien Software OpenSSL.[95] Diese Implementierung verfolgte den Zweck, eine bereits hergestellte Verbindung zwischen Server und Client aufrecht zu erhalten, indem der Kommunikationspartner (zB Mail-Server) Datenpakete mit beliebigem Inhalt (Payloads) an den anderen versendet. Der Empfänger retournierte nach Erhalt dieselben Daten wieder an den Sender. Die Schwachstelle bestand darin, dass Datenpakete nicht auf ihre tatsächliche Größe überprüft wurden, weshalb Angreifer in der Lage waren, Daten aus dem Arbeitsspeicher auszulesen.

2.2.2.6. Gefahren durch alternative „Hacking“-Techniken

Im Rahmen von Social-Engineering-Angriffen werden im Gegensatz zum „klassischen“ Hacking keine technischen Zugangsbarrieren im Computersystem umgangen, sondern durch Täuschung gezielt menschliche Schwächen oder Eigenschaften (bspw Gutgläubigkeit,

---

89 *Winterer*, Windows 7 Sicherheit, 97 f.
90 *Ziegler*, Web Hacking, 98 ff.
91 <heise.de/ct/artikel/Das-Sicherheitsloch-285320.html> (13.10.2014); ausführlich dazu siehe *Ziegler*, Web Hacking, 157 ff.
92 *Kammermann*, CompTIA Network+[5], 318.
93 *Spenneberg*, Linux-Firewalls mit iptables & Co: Sicherheit mit Kernel 2.4 und 2.6 für Linux-Server und –Netzwerke (2006) 67 f; *Ziegler*, Web Hacking, 158.
94 Vgl dazu den Eintrag zum Heartbleed-Exploit der Vulnerability-Datenbank MITRE.org <cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160> (14.10.2014).
95 <heise.de/security/artikel/So-funktioniert-der-Heartbleed-Exploit-2168010.html> (14.10.2014).

Unsicherheit, Bestechlichkeit) ausgenutzt, um sich Zugang zum Zielsystem zu verschaffen.[96] Dabei sind insb soziale Netzwerke oder Suchmaschinen im Internet als Informationsquelle von besonderer Bedeutung.[97] Social Engineering wird für Angreifer zunehmend wichtiger, weil verschiedene Maßnahmen (zB Passwörter mit 128 Bit-Verschlüsselungen oder Behebungen bekannter Schwachstellen durch entsprechende Software-Updates) das Eindringen in fremde Computersysteme erschweren oder verunmöglichen.[98]

Eine weitere Alternative ist „Google-Hacking". Dieser Begriff beschreibt entgegen dem ersten Anschein nicht das „Hacken" der Internet-Suchmaschine selbst,[99] sondern die Eingabe spezieller Suchbegriffe (zB intitle:"index of" passwd). Mithilfe dieser Parameter können die auf einem Server ungeschützt gespeicherten Dateien (Zugangs- oder Kundendaten, vertrauliche Informationen udgl) abgerufen werden.[100]

2.2.3. Viren, Würmer und andere Malware

Obwohl der Einsatz von Schadsoftware für die vorliegende Arbeit nicht von zentraler Bedeutung ist, erscheint es aufgrund der zunehmenden Bedrohung „hybrider Schädlinge" sinnvoll,[101] auf technische Grundlagen einzugehen. Der Begriff „Malware" bezeichnet bösartige Computerprogramme, deren Funktionsweisen vom betroffenen Benutzer unerwünscht sind.[102] Dieser Überbegriff erfasst neben Viren, Würmern und trojanischen Pferden auch Schadprogramme mit speziellen Eigenschaften und Funktionen (zB Ransomware[103], Spyware[104]).

2.2.3.1. Computervirus

Computerviren stellen aus technischer Sicht Befehlsfolgen dar, die Wirtsprogramme zur Ausführung benötigen und sich an diese anheften.[105] Wird das befallene Wirtsprogramm gestartet, verbreitet sich der Virus auf noch nicht infizierte Dateien. Klassische Computerviren sind heutzutage allerdings kaum mehr im Einsatz.

---

96 *Ziegler*, Web Hacking, 125 ff.
97 *Ziegler*, Web Hacking, 127.
98 *Winterer*, Windows 7 Sicherheit, 72 ff.
99 *NetSecure-IT*, Google Hacking, 2 <whitepaper.netsecure-it.de/Whitepaper_Google_Hacking.pdf> (3.12.2014).
100 *NetSecure-IT*, Google Hacking, 3 ff.
101 Hybride Schädlinge sind Kombinationen einzelner Malware-Arten; vgl dazu <sans.edu/research/security-laboratory/article/hybrid-threats-did> (1.12.2014).
102 *Winterer*, Windows 7 Sicherheit, 15.
103 Diese Schadsoftware verschlüsselt Daten auf den Rechnern der Opfer, um Lösegeld zu erpressen; vgl dazu <itwissen.info/definition/lexikon/Ransomware-ransomware.html> (1.12.2014).
104 Der Begriff Spyware bezeichnet Software zum Ausspionieren von Daten (zB Zugangsdaten); siehe <itwissen.info/definition/lexikon/Spyware-spyware.html> (1.12.2014).
105 *Eckert*, IT-Sicherheit[6], 53 f.

2.2.3.2. Computerwurm

Computerwürmer sind Schadprogramme, die im Gegensatz zu Viren kein Wirtsprogramm benötigen. Würmer verbreiten sich in kurzer Zeit über aktive Verbindungen im Internet, indem sie gezielt Schwachstellen in Anwendungen (zB Buffer-Overflows) nutzen. [106] Das Computernetzwerk der US-Raumfahrtbehörde wurde 1989 im Zuge von Protesten gegen Atomtests mit dem Computerwurm „WANK“[107] infiziert.[108]

2.2.3.3. Trojanisches Pferd

Als Trojanische Pferde (kurz Trojaner) werden Schadprogramme bezeichnet, die idR als nützliche Anwendungen getarnt sind und daher von AnwenderInnen zumeist freiwillig installiert werden.[109] Im Unterschied zu Viren und Würmern sind diese Schädlinge grundsätzlich nicht in der Lage, sich selbständig zu verbreiten. Heimlich eingeschleuste Keylogger-Trojaner protokollieren bspw Tastatureingaben und filtern Wörter, die als Zugangscodes geeignet erscheinen. Andere überprüfen und analysieren den gesamten Netzwerkverkehr, um etwa Passwörter zu ermitteln (Sniffer). Remote-Access-Trojaner (kurz RAT) werden bspw eingesetzt, um die Kontrolle über fremde Rechner zu erlangen.[110]

2.2.4. Denial-of-Service

Denial-of-Service (kurz DoS) bezeichnet die Nichtverfügbarkeit eines Dienstes (zB Web- oder E-Mail-Server), der grundsätzlich verfügbar sein sollte.[111] Solche Dienstblockaden können einerseits durch Wartungsarbeiten, Stromausfälle, Hardware- bzw Softwarefehler, aber auch durch gezielte Angriffe verursacht werden.

2.2.4.1. DoS- und DDoS-Angriffe

DoS-Attacken sind Angriffe auf die Verfügbarkeit von Diensten.[112] Dienstverweigerungen können bspw durch Buffer-Overflows herbeigeführt werden. Der Begriff „DDoS“ bezeichnet im Unterschied dazu verteilt (dh durch mehrere Rechner) ausgeführte Angriffe auf Computersysteme. Im konkreten Zusammenhang werden Ressourcen eines Zielsystems (zB Prozessorleistung, Arbeitsspeicher, Bandbreite) durch eine Flut von Datenpaketen derart überbeansprucht, sodass dieses zunächst verlangsamt und letztlich abstürzt.[113]

---

[106] *Winterer*, Windows 7 Sicherheit, 122 ff.
[107] Abkürzung für Worm Against Nuclear Killers.
[108] <en.wikipedia.org/wiki/WANK_(computer_worm)> (1.12.2014).
[109] *Winterer*, Windows 7 Sicherheit, 145 ff.
[110] *Winterer*, Windows 7 Sicherheit, 154 f.
[111] <itwissen.info/definition/lexikon/denial-of-service-DoS-DoS-Attacke.html> (27.9.2014).
[112] *Kappes*, Netzwerk- und Datensicherheit[2], 249 ff.
[113] *Studer*, Netzwerkmanagement und Netzwerksicherheit: Ein Kompaktkurs für Praxis und Lehre (2010) 110.

2.2.4.1.1. Mail-Bombing

Beim „klassischen“ Mail-Bombing wird ein Empfänger mit tausenden gleichlautenden E-Mails bombardiert, um das Postfach zu blockieren bzw den Mail-Server „lahmzulegen“.[114] Eine „Mail-Bombe“ besteht aus einem einzigen E-Mail. Die Besonderheit besteht darin, dass dieses Mail die Adresse des Empfängers hundert- oder tausendfach als BCC-Empfänger enthält. Im Gegensatz dazu bezeichnet der Begriff „Spamming“ das unaufgeforderte Versenden von E-Mails (zB Werbung) an eine Vielzahl von Empfängern.[115]

2.2.4.1.2. Broadcast Storms

Mit der Durchführung von Broadcast-Stürmen (zB „Smurf-Attacken“) wird das Ziel verfolgt, sämtliche Rechner im Netzwerk anzusprechen, um Überlastungen oder Abstürze des Routers herbeizuführen.[116] Im Zuge solcher Angriffe werden ICMP-Pakete (Ping-Anfragen) an die Broadcast-Adresse[117] des „gegnerischen“ Netzwerks gesendet.[118] Als Absender wird allerdings die IP-Adresse des Angriffsziels eingetragen (IP-Spoofing). Der angesprochene Router leitet daraufhin die empfangene Anfrage an alle Geräte innerhalb des Netzwerks weiter und erhält sämtliche Antworten der Rechner, wodurch es zu den bereits erwähnten Überlastungen und Abstürzen kommt.

2.2.4.1.3. TCP-Syn-Flooding

SYN-Flooding-Angriffe nutzen den „Drei-Wege-Handshake“ zwischen Client und Server beim Aufbau einer TCP-Verbindung. Unter normalen Umständen sendet der Client ein SYN-Paket[119] an den Server, der ein SYN-ACK-Paket retourniert. Der Client bestätigt dieses wiederum mit dem ACK-Paket[120], um eine Verbindung zum Server herzustellen. Bei SYN-Flooding-Attacken werden zwar die Synchronisierungsanfragen vom Angreifer versendet, der Erhalt des SYN-ACK-Pakets allerdings nicht bestätigt, weshalb zahlreiche „halboffene“ Verbindungen zum Zielsystem bestehen und andere Clients abgewiesen werden.[121]

2.2.4.1.4. Reflektierte Angriffe

Bei reflektierten Attacken (kurz DRDoS) wird das Zielsystem nicht direkt angegriffen, sondern eine Vielzahl fremder Computer benutzt, um das System mit sinnlosen Anfragen zu

---

114 *Studer*, Netzwerkmanagement und Netzwerksicherheit, 110.
115 *Eckert*, IT-Sicherheit[6], 78 f.
116 *Studer*, Netzwerkmanagement und Netzwerktechnik, 111.
117 Im Unterschied zum Unicast werden beim Broadcast sämtliche Rechner eines Netzwerks angesprochen.
118 *Studer*, Netzwerkmanagement und Netzwerksicherheit, 112.
119 SYN (synchronize) bezeichnet die Synchronisierungsanfrage.
120 Die Abkürzung ACK (acknowledgement) bezeichnet die Bestätigung des Kommunikationspartners.
121 *Ziegler*, Web Hacking, 114 f; *Studer*, Netzwerkmanagement und Netzwerksicherheit, 112 ff.

überfluten.[122] Dabei wird die IP-Adresse des Angreifers mittels IP-Spoofing verschleiert und stattdessen die Adresse des Zielrechners an die „angreifenden" Computer übermittelt, wodurch das Opfersystem sämtliche Antworten erhält und letztlich abstürzt.

2.2.4.2. Bedrohung durch Botnetze

Ein Roboternetzwerk (kurz Botnetz) ist ein Zusammenschluss infizierter Computer („Zombies"), die idR durch C&C-Server[123] kontrolliert und ferngesteuert werden.[124] Die Betreiber von Botnetzen werden „Bot-Master" genannt. „Bot-Herding" bezeichnet hingegen die Generierung fernsteuerbarer „Zombies" durch sog „Bot-Herder".[125] Mithilfe der eingeschleusten Schadsoftware erlangt der Angreifer die Kontrolle über die befallenen Geräte und kann diese an das Netzwerk anbinden. Solche Netze umfassen tausende bzw Millionen fernsteuerbarer Rechner. Die Einsatzbereiche von Botnetzen sind vielfältig. Neben der Ausführung von DDoS-Attacken dienen Botnetze auch der Versendung von Spam- oder Phishing-Mails.[126] Darüber hinaus sind die Daten der gekaperten Rechner selbst gefährdet.

2.3. Zusammenfassung

Neben „klassischen" Hacking-Techniken, die in erster Linie Schwachstellen in Programmen ausnutzen, stehen einem Angreifer weitere Methoden zur Verfügung. Dabei werden insb menschliche „Schwachstellen" (Social-Engineering) oder Nachlässigkeiten im Bereich der Datenverwaltung (Google-Hacking) gnadenlos ausgenutzt. (D)DoS-Attacken verfolgen im Unterschied zu klassischen Hacking-Angriffen das primäre Ziel, einen Rechner oder Internetdienst zum Absturz zu bringen bzw erheblich zu überlasten.

---

[122] *Ziegler*, Web Hacking, 114.
[123] Abkürzung für Command-and-Control-Server.
[124] *Eckert*, IT-Sicherheit[6], 75 ff.
[125] *Bu/Bueno/Kashyap/Wosotowsky*, Das neue Zeitalter der Botnets, 3 ff <mcafee.com/de/resources/white-papers/wp-new-era-of-botnets.pdf> (23.11.2014).
[126] *Winterer*, Windows 7 Sicherheit, 187 f.

3. Das Online-Phänomen „Hacktivismus“

3.1. Der Begriff

Der Begriff „Hacktivismus“ (Wortkombination aus „Hack“ und „Aktivismus“) bezeichnet die Verwendung von Computern oder Netzwerken als Protestmittel, um politische oder soziale Ziele durchzusetzen.[127]

3.2. Definitionen und Einordnungsprobleme

Denning unterscheidet hinsichtlich politisch motivierter Online-Aktivitäten zwischen Aktivismus, Hacktivismus und Cyber-Terrorismus.[128] Die Autorin definiert Hacktivismus als das Zusammentreffen von Hacking und Aktivismus, wobei Hacking iSv ungewöhnlicher und oftmals illegaler Nutzung von Computersystemen sowie die Verwendung spezieller Tools (Hacking-Tools) zu verstehen ist.[129] Als Erscheinungsformen führt sie insb virtuelle Sit-Ins, Mail-Bomben, Hacking, sowie den Einsatz von Malware an.[130]

Das deutsche Bundeskriminalamt definiert Hacktivismus folgendermaßen: „Hacktivismus setzt sich aus den Konzepten des Hackings und des Aktivismus zusammen. Die Schnittstelle beider Konzepte erklärt hacktivistische Ausrichtungen. Es handelt sich demnach um ideologisch, sozial und/oder politisch motivierte Aktionen unter Nutzung von Hacking-/IuK-Tools. Computer und Netzwerke sind Tatmittel und Angriffsziele zugleich. Sie werden als Protestmittel zur Verdeutlichung politischer und/oder gesellschaftlicher Ideologien eingesetzt. Die Taten sind nicht profitorientiert, es geht nicht um das missbräuchliche Erlangen von materiellem und/oder finanziellem Gewinn.“[131]

Vegh gliedert soziale Protest-Bewegungen im Internet in 3 Ebenen.[132] In der ersten Ebene (Awareness/Advocacy) nutzen soziale Online-Bewegungen das Internet, um breite Aufmerksamkeit für bestimmte (politische) Anliegen zu erlangen (zB durch die Verbreitung von Informationen auf Webseiten).[133] Die zweite Ebene (Organization/Mobilization) umfasst demgegenüber Aktivitäten, die insb der Vorbereitung von Online- und Offline-Protesten dienen (zB Rekrutierung von Teilnehmern für virtueller Sit-Ins oder die Planung und Koordinierung

[127] <de.wikipedia.org/wiki/Hacktivismus> (22.9.2014).
[128] Siehe dazu *Denning*, Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy, 2 <faculty.nps.edu/dedennin/publications/Activism-Hacktivism-Cyberterrorism.pdf> (23.9.2014).
[129] *Denning*, Activism, Hacktivism, and Cyberterrorism, 15.
[130] *Denning*, Activism, Hacktivism, and Cyberterrorism, 15 ff.
[131] *Bundeskriminalamt*, Hacktivisten: Abschlussbericht zum Projektteil der Hellfeldbeforschung, 7 <bka.de/> (1.2.2015).
[132] *Vegh*, Classifying Forms of Online Activism: The Case of Cyberprotests against the World Bank, in McCaughey/Ayers (Hrsg), Cyberactivism: Online Activism in Theory and Practice (2003) 71 (72 ff).
[133] *Vegh* in McCaughey/Ayers, Cyberactivism, 72 ff.

von Straßenblockaden).[134] Hacktivismus wird der dritten Ebene (Action/Reaction) zugeordnet.[135] Darunter sind direkte Protest-Aktionen im Internet (zB virtuelle Sitzblockaden, Web-Defacement oder E-Mail-Kampagnen) zu verstehen.[136]

Jordan/Taylor unterteilen Hacktivismus grob in die Kategorien „Mass-Action-Hacktivism" und „Digitally-Correct-Hacktivism".[137] Erstere Strömung bezeichnet Massenproteste im Internet (zB virtuelle Sit-Ins), an denen tausende InternetnutzerInnen mitwirken. Im Gegensatz dazu verfolgen Vertreter der zweiten Strömung das Ziel, den weltweiten Informationsfluss ohne Einschränkungen (zB durch staatliche Internetzensur oder -überwachung) zu gewährleisten, indem entsprechende Software bzw alternative Kanäle geschaffen werden, um staatliche Maßnahmen zu umgehen.

Möhlen vermeidet hingegen die Verwendung des schwer zu definierenden Begriffes „Hacktivismus". [138] Seines Erachtens bietet das Internet zahlreiche digitale Protestformen, die keine Hacking-Kenntnisse voraussetzen.

3.3. Internetbasierte Protestmethoden im Überblick

3.3.1. Online-Petitionen und Boykottaufrufe in sozialen Netzen

Boykottaufrufe in sozialen Netzwerken, die durch „Liken" bzw „Teilen" mit einem Maus-Klick unterstützt werden können, sind neben Online-Petitionen häufig verwendete Protestmittel im Internet.[139] Diese beiden Protestformen wurden im Zuge einer Online-Kampagne gegen die widrigen Arbeitsbedingungen von Leiharbeitern des Online-Händlers Amazon miteinander verknüpft.[140]

3.3.2. Shitstorm

Der Duden beschreibt das Online-Phänomen Shitstorm als „Sturm der Entrüstung in einem Kommunikationsmedium des Internets, der zum Teil mit beleidigenden Äußerungen einhergeht".[141] Dabei richten mehrere tausend NutzerInnen in kurzer Zeit teils aggressive, beleidigende, oder bedrohende Äußerungen gegen Unternehmen, staatliche Einrichtungen,

---

134 *Vegh* in McCaughey/Ayers, Cyberactivism, 74 f.
135 *Vegh* in McCaughey/Ayers, Cyberactivism, 75 ff.
136 *Vegh* in McCaughey/Ayers, Cyberactivism, 85.
137 *Jordan/Taylor*, Hacktivism and Cyberwars: Rebels with a Cause (2004) 67 ff.
138 *Möhlen*, Gibt es ein Recht auf politischen Online-Protest?, in Landler/Parycek/Kettemann (Hrsg), Netzpolitik in Österreich: Internet. Macht. Menschenrechte. Abschlussbericht 2013 (2013) 97 (98).
139 *Möhlen* in Landler/Parycek/Kettemann, Netzpolitik in Österreich, 97 (100).
140 Siehe dazu etwa <kurier.at/lebensart/technik/amazon-skandal-verursacht-protestwelle-und-boykott-aufrufe-im-netz/3.671.631> (5.10.2014).
141 <duden.de/rechtschreibung/Shitstorm> (5.10.2014).

oder Einzelpersonen.[142] Als Auslöser kommen neben Berichten klassischer Medien (zB Zeitung, Fernsehen) auch Meldungen in sozialen Netzwerken in Betracht. Im Rahmen der Debatte zwischen Ministerin *Heinisch-Hosek* und Musiker *Gabalier* zur Causa „Bundeshymne" wurden zahlreiche beleidigende und drohende Äußerungen auf der Facebook-Seite der Ministerin „gepostet".[143]

3.3.3. Online-Blackout

Im Zuge von Netz-Demonstrationen werden sog „Online-Blackouts" durch die Betreiber von Webseiten selbst verursacht, indem sie die Seiten-Inhalte für die Dauer des Protests verändern oder den Internetdienst beenden.[144] Als Beispiel kann der Blackout der englischsprachigen Online-Enzyklopädie Wikipedia genannt werden.[145] Im Zuge des Protestes wurden Webseiten-Inhalte durch Kommentare und schwarzer Hintergrundfarbe ersetzt, um gegen die Umsetzung der Antipiraterie-Abkommen SOPA und PIPA zu demonstrieren.

3.3.4. Online-Sitzblockaden

Online-Sitzblockaden, auch virtuelle Sit-Ins genannt, stellen aus technischer Sicht DDoS-Angriffe dar. Virtuelle Sit-Ins verfolgen das Ziel, Web-Server staatlicher Einrichtungen oder einflussreicher Unternehmen durch das Versenden massenhafter Anfragen zum Absturz zu bringen, um soziale oder politische Anliegen durchzusetzen.[146] Die Besonderheit derartiger DDoS-Angriffe liegt darin, dass tausende bzw zehntausende Online-Demonstranten an Attacken teilnehmen oder Rechner freiwillig einem Botnetz zur Verfügung stellen.[147] Mitglieder der amerikanischen Aktivistengruppe „Electronic-Disturbance-Theater" (kurz EDT) organisierten und koordinierten Angriffe auf Web-Server mexikanischer Finanzinstitute.[148] Um derartige Online-Sitzblockaden überhaupt durchführen zu können, werden automatisierte DDoS-Tools entwickelt und im Internet zur Verfügung gestellt.[149] Programmierer der Hacktivisten-Gruppierung EDT entwickelten etwa das Tool „Flood-Net", um damit automatisierte Angriffe auf mexikanische Web-Server durchzuführen, indem diese Software den „Reload-Befehl"[150] im Abstand von wenigen Sekunden selbständig ausführte.[151]

---

142 <big-social-media.de/news_publikationen/meldungen/2012_06_04_Shitstorm.php> (5.10.2014).
143 <derstandard.at/2000002393084/Sexismus-Shitstorm-gegen-Heinisch-Hosek> (6.10.2014).
144 *Möhlen* in Landler/Parycek/Kettemann, Netzpolitik in Österreich, 97 (100).
145 <futurezone.at/netzpolitik/diese-seiten-machen-beim-internet-blackout-mit/24.574.845> (5.10.2014).
146 <de.wikipedia.org/wiki/Online-Demonstration> (6.10.2014).
147 *Bundeskriminalamt*, Hacktivisten, 28.
148 <heise.de/tp/artikel/1/1461/1.html> (6.10.2014).
149 *Bundeskriminalamt*, Hacktivisten, 29.
150 Dieser Befehl hat grundsätzlich die Funktion, eine aktuelle Version der aufgerufenen Webseite vom Server anzufordern.
151 <heise.de/tp/artikel/1/1461/1.html>.

3.3.5. Web-Defacements

Der Begriff „Defacement“ (auch Web-Graffiti genannt) bezeichnet das unberechtigte Verändern oder Löschen von Webseiten-Inhalten.[152] Im Rahmen politisch motivierter Defacements werden durch den Einsatz unterschiedlicher Web-Hacking-Techniken (zB SQL-Injection, Brute-Force, XSS) idR die sichtbaren Inhalte einer Seite (zB Texte, Grafiken, Animationen udgl) verunstaltet und durch politische Botschaften ersetzt.[153] Informationen zu Defacement-Angriffen werden auf Online-Plattformen (zB Zone-H)[154] dokumentiert und archiviert.

3.3.6. Doxing

Der Begriff „Doxing“[155] beschreibt die internetbasierte Suche nach persönlichen Informationen (Namen, Telefonnummern, E-Mail-Adressen, Bilder usw) von Personen und deren Veröffentlichung auf Online-Plattformen (zB Pastebin[156]).[157] Die Methoden zur Erlangung dieser Informationen sind vielfältig, weshalb neben Suchabfragen in öffentlich zugänglichen Online-Datenbanken und das Durchsuchen von Facebook-Profilen, auch Hacking oder Social-Engineering als Möglichkeiten angeführt werden können.[158]

3.4. Abgrenzungen

3.4.1. Internet-Aktivismus

Organisationen (zB AVAAZ, Greenpeace), aber auch einzelne Netz-Aktivisten (zB Blogger) verwenden Internetdienste idR zur Sammlung, Aufbereitung und Verbreitung von Information, um die Öffentlichkeit auf politische oder soziale Missstände hinzuweisen.[159] Im Gegensatz zum Hacktivismus wird das Internet idR legal als Informations- und Kommunikationsmedium genutzt.[160]

3.4.2. Online-Kriminalität

Im Unterschied zu Cyber-Kriminellen, die mit Angriffen zumeist finanzielle Interessen verfolgen (zB Phishing oder Bestellbetrug), agieren Hacktivisten zumeist nicht profitorientiert, sondern

---

[152] <de.wikipedia.org/wiki/Defacement> (7.10.2014); *Bundeskriminalamt*, Hacktivisten, 26 f.
[153] *Winterer*, Windows 7 Sicherheit, 52 ff.
[154] Siehe dazu die Webseite der Online-Plattform Zone-H <zone-h.org/archive> (7.10.2014).
[155] Kurzform für „document tracing“.
[156] <pastebin.com> (7.10.2014).
[157] *Paget*, Hacktivismus: Das Internet ist das neue Medium für politische Stimmen, 15 <mcafee.com/de/resources/white-papers/wp-hacktivism.pdf> (20.9.2014); <gohacking.com/what-is-doxing-and-how-it-is-done/> (8.10.2014).
[158] <en.wikipedia.org/wiki/Doxing> (8.10.2014).
[159] *Denning*, Activism, Hacktivism and Cyberterrorism, 3ff.
[160] *Bundeskriminalamt*, Hacktivisten, 23.

versuchen, politische oder soziale Ideologien durchzusetzen und erlangen dadurch zumeist breite Aufmerksamkeit.[161] Politisch motivierte Cyber-Aktionen werden zum Teil im Vorfeld angekündigt (zB mittels Videobotschaften auf YouTube)[162] und sind daher für Opfer bereits vor den tatsächlichen Angriffen erkennbar.[163]

Eine weitere Besonderheit im Zusammenhang mit „hacktivistischen" Online-Aktivitäten besteht darin, dass bestimmte Angriffsziele ausgewählt und attackiert werden (sog „Targeted-Attacks").[164] Cyber-Kriminelle sind hingegen bei der Auswahl ihrer Opfer, mit Ausnahme von Cyber-Spionage, grundsätzlich nicht wählerisch (sog „Opportunistic-Attacks").

3.4.3. Cyber-Terrorismus und Cyber-Krieg

Online-Aktionen von Hacktivisten werden oftmals als Cyber-Terrorismus missverstanden.[165] Im Gegensatz zu Hacktivisten nutzen Terroristengruppen das Internet hauptsächlich als Kommunikationsmedium zur Radikalisierung und Rekrutierung von Jugendlichen.[166]

Die Bedrohung von Computersystemen kritischer Infrastrukturen iSd ErwG 4 Richtlinie 2013/40/EU des Europäischen Parlaments und des Rates vom 12.8.2013 über Angriffe auf Informationssysteme zur Ersetzung des Rahmenbeschlusses 2005/222/JI des Rates[167] wird derzeit noch kontrovers diskutiert.[168] Als Angriffsziele von Cyber-Terroristen kommen etwa Computersysteme von Energie- oder Wasserversorgungseinrichtungen (zB Atomkraftwerke) in Betracht, deren Störungen oder Ausfälle erhebliche Schäden verursachen können.

Der Begriff „Cyber-Krieg" (auch Cyber-War) bezeichnet hingegen die Nutzung des Internet zur Unterstützung konventioneller Kriegsführung von Staaten.[169] Diese Online-Aktivitäten lassen sich von „hacktivistischen" Aktionen dadurch abgrenzen, dass derartige Attacken idR von

---

[161] *Bundeskriminalamt*, Cybercrime Report 2013, 14 ff; *Bundeskanzleramt*, Bericht Cyber Sicherheit 2014, 6 <bka.gv.at/DocView.axd?CobId=55935> (8.10.2014).

[162] Vgl dazu etwa die Botschaft von Anonymous, die vor der geplanten Operation Payback auf YouTube veröffentlicht wurde <youtube.com/watch?v=fL3_4tsG_Ig> (8.10.2014).

[163] <ikarussecurity.com/at/support/infos-tipps/sicherheitsempfehlungen/hacking-praevention-und-handling/> (9.10.2014).

[164] <sicherheitskultur.at/Angreifer_im_Internet.htm> (9.10.2014).

[165] *Bundeskriminalamt*, Hacktivisten, 22.

[166] *Bundeskriminalamt*, Hacktivisten, 22.

[167] Richtlinie 2013/40/EU des europäischen Parlaments und des Rates vom 12. August 2013 über Angriffe auf Informationssysteme zur Ersetzung des Rahmenbeschlusses 2005/222/JI des Rates, ABl L 2013/218, 8; im Folgenden RL 2013/40/EU.

[168] *Bundeskriminalamt*, Hacktivisten, 22.

[169] *Schumacher*, Vom Cyber-Kriege, in Sambleben/Schumacher (Hrsg), Informationstechnologie und Sicherheitspolitik: Wird der dritte Weltkrieg im Internet ausgetragen? (2012) 2 (19 f).

Regierungen beauftragt werden.[170] Im konkreten Zusammenhang ist anzumerken, dass staatlich beauftragte Cyber-Angriffe in praxi meist schwer nachweisbar sein werden.[171]

3.5. Zusammenfassung

Das Internet bietet Aktivisten zahlreiche Möglichkeiten, den gesamten Protest im Internet durchzuführen (zB Online-Petitionen, E-Mail-Kampagnen). Unter dem Begriff „Hacktivismus" sind hauptsächlich politisch motivierte Cyber-Angriffe sowie die Entwicklung und Verbreitung spezieller Software im Vorfeld solcher Attacken zu verstehen. Die öffentlichkeitswirksamsten Erscheinungsformen sind jedenfalls Defacement- und DDoS-Attacken.

[170] *Bundeskriminalamt*, Hacktivisten, 25; <spiegel.de/politik/ausland/hackerangriffe-usa-beschuldigen-china-der-cyber-spionage-a-898446.html> (9.10.2014).

[171] <heise.de/security/meldung/Stuxnet-Gemeinschaftsprojekt-der-USA-und-Israels-1170175.html> (9.10.2014).

4. Die Akteure: Hacker, Cracker oder Hacktivisten?

4.1. Der Begriff „Hacker“

Die Web-Definition beschreibt einen Hacker als jemanden, „der in fremde Computersysteme eindringen kann und zugleich Teil einer entsprechenden Szene ist“.[172] Im Folgenden werden einzelne Gruppierungen innerhalb der Hacker-Szene näher beleuchtet.

4.1.1. Phreaker

Vorläufer der heutigen Computer-Hacker werden als Phreaker[173] bezeichnet. Deren Tätigkeit bestand hauptsächlich darin, Telefonverbindungen derart zu manipulieren, um kostenlos zu telefonieren.[174] Unter dem Pseudonym „Captain Crunch“ entdeckte der Amerikaner *John T. Draper*, dass Spielzeugpfeifen das erforderliche Signal wiedergeben konnten, um den Gebührenzähler zu deaktivieren („Blue-Boxing“).[175] Diese traditionellen Methoden sind in der Phreaker-Szene zunehmend in den Hintergrund getreten.

4.1.2. Klassische Hacker

Klassische Hacker dringen idR aus Neugierde in fremde Computer ein und besitzen tiefe Grundlagenkenntnisse in den Bereichen Computer- und Netzwerktechnik.[176] Diese Computerspezialisten identifizieren sich mit den Werten der sog „Hacker-Ethik“, welche die Grenzen und die Motivation des Hackens beschreibt, dh Schädigungen der Opfer werden von einem klassischen Hacker abgelehnt.[177] Allerdings ist anzumerken, dass klassische Hacker im Zusammenhang mit Cyber-Angriffen nur eine untergeordnete Rolle spielen.[178]

4.1.3. Cracker

Der Begriff „Cracker“ wurde etwa Mitte der 1980er Jahre von Teilen der Hackerszene benutzt, um ihre Abneigung gegenüber einzelnen Gruppierungen zum Ausdruck zu bringen, die mit Schädigungsabsicht in Systeme eindrangen.[179] Diese Angreifer werden auch als Crasher

---

[172] <de.wikipedia.org/wiki/Hacker>.
[173] Wortkombination aus „Phone“ und „Freak“.
[174] <itwissen.info/definition/lexikon/Phreaking-phreaking.html> (13.11.2014); M*oschitto/Sen*, Hackerland: das Logbuch einer Szene[4] (2011) 65 ff.
[175] *Moschitto/Sen*, Hackerland[4], 69; *Winterer*, Windows 7 Sicherheit, 47.
[176] <catb.org/jargon/html/H/hacker.html> (13.11.2014); *Pfister*, Hacking in der Schweiz: im Spiegel des europäischen, des deutschen und des österreichischen Computerstrafrechts (2008) 90 f.
[177] <catb.org/jargon/html/H/hacker-ethic.html> (13.11.2014); vgl dazu auch die ethischen Grundsätze der deutschen Hackergruppe mit dem Namen Chaos Computer Club <ccc.de/de/hackerethik> (13.11.2014).
[178] *Bundeskanzleramt*, Bericht Cyber Sicherheit 2014, 6.
[179] <catb.org/jargon/html/C/cracker.html> (30.11.2014); *Pfister*, Hacking in der Schweiz, 92.

bezeichnet.[180] Softwarecracker sind jene Akteure, die Kopierschutzmechanismen in Programmen (zB Computerspielen) entschlüsseln und Raubkopien erstellen.[181]

4.1.4. Script-Kiddies

Script-Kiddies sind meist junge und unerfahrene Computernutzer, welche durch die Verwendung von Anleitungen (sog „Tutorials“) oder bereits fertiggestellter Hacking-Tools überhaupt erst in der Lage sind, in fremde Systeme einzudringen.[182] Vertreter dieser Szene arbeiten im Gegensatz zu klassischen Hackern und Crackern idR unprofessionell und werden gerade auch deswegen von diesen verachtet.[183] Als leitende Motive von Script-Kiddies können insb Geltungsdrang, Langeweile und Neugierde angeführt werden.[184] Die Cyber-Angriffe dieser „Möchtegern-Hacker“ sind als besonders gefährlich einzustufen, weil sie das Ausmaß eines möglichen Schadens meist nicht vorhersehen können.[185]

4.1.5. Hacker im Bereich der Computersicherheit

Abhängig von Motivation und Gesetzestreue werden Hacker in die Kategorien „White-, Black- und Grey-Hat“ eingeteilt.[186] White-Hat-Hacker, auch Ethical-Hacker genannt, agieren gesetzeskonform, indem sie bspw Penetration-Tests im Auftrag von Kunden durchführen. Black-Hats handeln im Unterschied dazu mit krimineller Energie und beabsichtigen die Zerstörung von Zielsystemen oder Daten. Grey-Hats sind hingegen nicht eindeutig als „gut“ oder „böse“ einzustufen.

4.2. Hacktivisten als besondere Akteure im Internet

Hacktivisten werden als politisch motivierte Hacker bzw als besondere Online-Akteure bezeichnet, die Cyber-Angriffe durchführen, um politische oder soziale Ziele durchzusetzen.[187]

Paget analysierte das Phänomen „Hacktivismus“ und beschäftigte sich vorwiegend mit den Akteuren dieser Szene.[188] Im Folgenden werden die von ihm beschrieben Kategorien im Überblick dargestellt.

---

[180] *Reindl-Krauskopf*, Computerstrafrecht im Überblick[2] (2009) 10.
[181] *Pfister*, Hacking in der Schweiz, 92 f; *Reindl-Krauskopf*, Computerstrafrecht[2], 10.
[182] *Spenneberg*, Linux-Firewalls, 52; *Winterer*, Windows 7 Sicherheit, 45; *Pfister*, Hacking in der Schweiz, 93.
[183] <catb.org/jargon/html/S/script-kiddies.html> (13.11.2014).
[184] *Spenneberg*, Linux-Firewalls, 52.
[185] *Winterer*, Windows 7 Sicherheit, 45.
[186] <de.wikipedia.org/wiki/Hacker_(Computersicherheit)>; vgl dazu auch *Winterer*, Windows 7 Sicherheit, 44; *NetSecure-IT*, Hackerdefinition, 4.
[187] *Pfister*, Hacking in der Schweiz, 93; *Bundeskanzleramt*, Cyber Sicherheit 2014, 6.
[188] Siehe dazu *Paget*, Hacktivismus, 4.

4.2.1. Anonymous

Anonymous ist eine international agierende Online-Bewegung ohne erkennbare Hierarchie, deren Mitglieder (kurz Anons) in erster Linie Cyber-Angriffe (zB DDoS- oder Defacement-Attacken) durchführen, um ihre Anliegen durchzusetzen.[189] Anonymous-Hacktivisten verwenden bspw Anonymisierungsdienste (zB TOR[190]), um die Identifikation von IP-Adressen für Gegner und Strafverfolgungsbehörden zu erschweren.[191] Dieses Kollektiv hat ihren Ursprung in einem Forum des Image-Boards „4chan".[192] Die Kommunikation erfolgt hauptsächlich über soziale Netzwerke (zB Twitter[193]). Daneben entstanden auch nationale bzw regionale Gruppierungen der Anonymous-Bewegung (zB AnonAustria, Anonymous-Salzburg), die vorwiegend nationale Ziele verfolgen.[194] Die Website des Altstadtverbandes Salzburg wurde bspw verunstaltetet, um im konkreten Fall zur Flüchtlingsaufnahme aufzufordern.[195] Die erste bekannte Online-Aktion des Hacktivisten-Kollektivs wird als Habbo-Raid[196] bezeichnet. Einige Teilnehmer folgten dieser Online-Aktion, um gegen die zu geringe Anzahl farbiger Figuren in Online-Spielen zu protestieren. Andere beteiligten sich hingegen nur aus Spaß.

Während des Projekts „Chanology" wurden Webseiten der Religionsgemeinschaft Scientology angegriffen und Straßenproteste durchgeführt.[197] Im Rahmen der „Operation Payback" erfolgten DDoS-Attacken auf Webseiten von Geldinstituten (zB PayPal, Visa, Mastercard).[198] Aktuelle Angriffsziele der Hacktivisten sind Facebook- und Twitter-Konten der Terrorgruppe IS, die vorwiegend zu Propaganda- und Rekrutierungszwecken genutzt werden.[199]

4.2.1.1. Verlauf einer Anonymous-DDoS-Attacke

Das IT-Sicherheitsunternehmen Imperva hat den Verlauf einer DDoS-Attacke des Anonymous-Kollektivs aus dem Jahr 2011 untersucht und dabei festgestellt, dass die analysierte Online-Aktion in 3 Phasen eingeteilt werden kann.[200] Im ersten Schritt, der sog

---

189 *Paget*, Hacktivismus, 4 ff.

190 Diese kostenlose Software ermöglicht den anonymen Internetzugang, indem Verbindungen zwischen Server und Clients verschlüsselt werden; <torproject.org/about/overview.html.en> (20.11.2014).

191 *Paget*, Hacktivismus, 22.

192 <de.wikipedia.org/wiki/Anonymous_(Kollektiv)> (22.11.2014); *Paget*, Hacktivismus, 4.

193 Vgl <twitter.com/youranonnews> (22.11.2014).

194 Siehe dazu <derstandard.at/1308680131769/Naechtlicher-Ueberfall-Anonymous-attackiert-Seiten-von-SPOe-und-FPOe> (23.11.2014); vgl auch die „Pressemitteilung" von Anonymous <pastebin.com/sHL5W4Rd> (23.11.2014).

195 <salzburg.com/nachrichten/salzburg/chronik/sn/artikel/anonymous-hackt-website-des-altstadtverbands-123551/> (23.11.2014).

196 Im Rahmen dieser Aktion wurde ein virtueller Hotel-Swimmingpool der Habbo-Spielecommunity mit dunkelhäutigen Avataren blockiert.

197 <chanology-wiki.info/anonymous#projekt-chanology> (23.11.2014).

198 *Paget*, Hacktivismus, 7 ff; <spiegel.de/netzwelt/web/operation-payback-hacker-grossangriff-auf-mastercard-visa-co-a-733520.html> (1.12.2014).

199 <twitter.com/hashtag/opisis> (1.12.2014); <anonhq.com/anonymous-hacktivists-strike-blow-isis/> (1.12.2014).

200 *Imperva*, Hacker Intelligence Summary Report: The Anatomy of an Anonymous Attack, 6 ff <imperva.com/download.asp?id=312> (1.12.2014).

„Rekrutierungs- und Kommunikationsphase“, die ungefähr 18 Tage andauerte, wurden Informationen über die aktuelle Unrechtssituation in sozialen Netzwerken (Facebook, YouTube und Twitter) verbreitet, um Unterstützer zu gewinnen. In der nächsten Phase wurde das Zielsystem auf Schwachstellen (zB Havij-Scanner)[201] abgetastet. Erst in der letzten Phase erfolgte die eigentliche DDoS-Attacke.

4.2.1.2. DDoS-Tools und deren Weiterentwicklung innerhalb der Szene

Anonymous-Aktivisten verwendeten im Rahmen der „Operation Payback“ das DDoS-Tool „LOIC“, um Zielserver mit sinnlosen Anfragen zu überlasten.[202] Durch die Aktivierung des sog „Hive-Mind-Modus“ konnten Rechner für die geplante Online-Aktion auch zur Verfügung gestellt werden. Diese Computer waren als Bestandteil eines (freiwilligen) Botnetzes mittels C&C-Server fernsteuerbar. Bei Angriffen auf die Webseiten des US-Justizministeriums wurde durch den Einsatz einer neuen „Waffe“ eine andere Taktik verfolgt.[203] Internetnutzer wurden zunächst auf eine mit Java-Script präparierte Webseite gelockt. Die Software namens „Mobile-LOIC“ begann sofort nach dem Aufruf der Seite mit der Versendung von Datenpaketen, weshalb Webseitenbesucher teilweise auch unfreiwillig an Attacken teilgenommen haben.

4.2.2. Cyberoccupier und Internetdissidenten

Paget bezeichnet Aktivisten in demokratischen Staaten, die das Internet grundsätzlich legal nutzen, als Cyberoccupier.[204] Internetdissidenten sind hingegen diejenigen, die ihre wahre Identität im politischen Kampf gegen totalitäre Regime nicht zum Spaß schützen, sondern dies vielmehr deswegen tun, um Haftstrafen oder Folterungen zu entgehen.[205]

Durch die Umleitung von Verbindungen konnten Mitglieder der Hacktivisten-Gruppe namens Telecomix den Internetzugang für mehrere Millionen NutzerInnen teilweise wieder herstellen, nachdem die ägyptische Regierung diesen blockierte, um Online-Protestbewegungen in sozialen Netzen (insb Facebook) unter Kontrolle zu bekommen.[206] Daneben wurden Vertreter dieser Hacker-Gruppe auch in Syrien aktiv, um alternative Kanäle zur Umgehung der staatlichen Netzüberwachung zu schaffen.[207]

---

[201] Der Havij-Scanner Version 1.17 ist ein automatisiertes SQL-Injection-Tool; siehe dazu <hack-tools.blackploit.com/2014/02/havij-117-automated-and-advanced-sql.html> (9.12.2014).
[202] <heise.de/ct/artikel/Operation-Payback-Proteste-per-Mausklick-1150151.html> (9.12.2014).
[203] <heise.de/security/meldung/Anonymous-neue-Waffe-1418014.html> (9.12.2014).
[204] *Paget*, Hacktivismus, 4.
[205] *Paget*, Hacktivismus, 24 f.
[206] *Paget*, Hacktivismus, 25; vgl dazu auch <derstandard.at/1295571047625/Wegen-Protesten-Aegyptische-Regierung-schaltet-Internet-ab> (9.12.2014); <spiegel.de/spiegel/a-791039.html> (9.12.2014).
[207] <spiegel.de/spiegel/a-791039-2.html> (9.12.2014).

4.2.3. Internetkrieger und Internetarmeen

Patriotische Hacker werden als Internetkrieger bezeichnet, die sog „Internetarmeen“ (zB SEA[208]) bilden.[209] Diese Zusammenschlüsse sind vor allem in totalitären Staaten aktiv und unterstützen Regime. Während der Operation Türkei[210] verunstaltete bspw eine Gruppe regierungsnaher türkischer Hacker die Startseite von „AnonPlus“, indem das Anonymous-Logo mit einem Hundekopf „verschönert“, und von den Angreifern eine verspottende Nachricht hinterlassen wurde.[211] Darüber hinaus sind Webseiten westlicher Medien beliebte Angriffsziele patriotischer Hacker.[212]

4.3. Zusammenfassung

Die Anonymous-Bewegung ist nicht erkennbar hierarchisch strukturiert. Die Mitglieder sind aber in sozialen Netzwerken miteinander verbunden und dem Anschein nach gut organisiert. Neben politisch motivierten Hackern zählen auch „normale“ InternetnutzerInnen zu den Unterstützern des Kollektivs, die sich aus politischer Überzeugung oder aus Spaß an einzelnen Online-Aktionen beteiligen. Cyber-Angriffe von Hacktivisten sind im Unterschied zu Attacken von Cyber-Kriminellen politisch motiviert.

[208] Siehe dazu die Webseite der Syrian-Electronic-Army <sea.sy/index/en> (9.12.2014).
[209] *Paget*, Hacktivismus, 27 f; *Bundeskanzleramt*, Cyber Sicherheit 2014, 6.
[210] Anonymous unterstützte dabei nationale Proteste gegen die Internetzensur mit Defacement- und DDoS-Angriffen auf Webseiten türkischer Behörden; vgl dazu <kurier.at/lebensart/technik/anonymous-attackiert-tuerkische-websites/715.651> (10.12.2014).
[211] *Paget*, Hacktivismus, 28.
[212] <sea.sy/Latest_Hacks_EN> (10.12.2014).

5. Computerstrafrechtliche Betrachtung

5.1. Vorbemerkungen

In diesem Kapitel werden die österreichischen Computerstrafdelikte (§§ 126a, 126b, 118a und 126c StGB) im Allgemeinen dargestellt. In weiterer Folge wird analysiert, ob bzw inwieweit diese Bestimmungen auf Web-Defacements und virtuelle Sit-Ins zur Anwendung gelangen. Im Anschluss wird auf die im Rahmen des StRÄG 2015 geplanten Änderungen der Delikte (§§ 118a, 126a und 126b) eingegangen.

5.2. Datenbeschädigung[213]

5.2.1. Allgemeines

5.2.1.1. Hintergrund der Regelung und internationale Vorgaben

Im Zuge des StRÄG 1987[214] wurden die ersten Computerstrafdelikte (§§ 126a und 148a) in das StGB eingeführt. Aufgrund der technischen Weiterentwicklung im IT-Bereich war die Einführung dieser Delikte im Hinblick auf den vielfach nicht oder unzureichend vorhandenen Strafschutz geboten.[215] Der Bestand von Daten wurde vor Inkrafttreten des § 126a durch § 49 DSG 1978[216] geschützt.[217]

Dieser Strafschutz war nach Ansicht des Justizausschusses jedoch nicht ausreichend, da einerseits der Unwert einer Datenbeschädigung durch die damalige Strafe nicht angemessen sanktioniert wurde und andererseits nur personenbezogene Daten vom Schutzbereich des DSG 1978 erfasst wurden.[218] Als weiterer Grund für die Einführung des § 126a wird ein Meinungsdiskurs in der Lehre und Rsp genannt, ob eine „reine" Datenbeschädigung von der Sachbeschädigung (§ 125) erfasst wird.[219] Kritiker des § 126a vertraten die Auffassung, dass die Beschädigung von Daten unter § 125 subsumiert werden könnte, weshalb die Einführung des Delikts der Datenbeschädigung ihres Erachtens nicht notwendig gewesen wäre.[220] Um eine Strafbarkeitslücke nicht aufkommen zu lassen, wurde § 126a nach Vorschlag des Justizausschusses in das StGB aufgenommen, da die Anwendbarkeit des § 125 zweifelhaft

---

213 § 126a idF BGBl I 109/2007.
214 Strafrechtsänderungsgesetz 1987, BGBl 605/1987.
215 JAB 359 BlgNR XVII. GP, 15; *Komenda/Madl* in Triffterer/Rosbaud/Hinterhofer (Hrsg), Salzburger Kommentar zum Strafgesetzbuch § 126a Rz 1 (Stand Juni 2013).
216 Bundesgesetz vom 18. Oktober 1978 über den Schutz personenbezogener Daten (Datenschutzgesetz – DSG), BGBl 565/1978.
217 *Komenda/Madl* in SbgK § 126a Rz 2.
218 JAB 359 BlgNR XVII. GP, 16.
219 *Komenda/Madl* in SbgK § 126a Rz 3; JAB 359 BlgNR XVII. GP, 16 f.
220 Vgl dazu *Seiler*, Kritische Anmerkungen zum StRÄG 1987 betreffend den Besonderen Teil des StGB, JBl 1989, 746 (751 ff); *Fuchs*, Zum Entwurf von Strafbestimmungen gegen die Computerkriminalität, RdW 1985, 330 (330).

erschien.[221] Mit der Einführung des § 126a wurden Daten im österreichischen Kernstrafrecht erstmalig als „eigenständiges schützenswertes Vermögensobjekt“ anerkannt.[222]

Als internationale Vorgaben sind Art 4 Convention on Cybercrime des Europarates[223] (im Folgenden CyCC) sowie Art 4 des Rahmenbeschlusses 2005/222/JI des Rates zum Schutz von Informationssystemen[224] (im Folgenden RB 2005/222/JI) zu beachten. Im Zuge der Umsetzung dieser Bestimmungen sah Österreich keine Notwendigkeit, den Tatbestand des § 126a inhaltlich zu verändern.[225] Im Zuge des StRÄG 2002 wurde die zuvor in § 126a Abs 2 aF[226] enthaltene Begriff „Daten“ durch die Begriffsbestimmung in § 74 Abs 2 ersetzt.[227] Mit dem StRÄG 2008[228] wurde die Begehung der Tat als Mitglied einer kriminellen Vereinigung als Qualifikation in § 126a Abs 2 aufgenommen.[229] Die bis September 2015 umzusetzende RL 2013/40/EU enthält in Art 5 leg cit eine entsprechende Regelung.[230]

5.2.1.2. Geschütztes Rechtsgut

Die Frage nach dem von § 126a geschützten Rechtsgut wird in der Lehre uneinheitlich beantwortet. Nach *Kienapfel* ist das Interesse am Fortbestand und an der Verfügbarkeit von Daten als spezieller Vermögenswert geschützt.[231] *Triffterer*, sich auf *Kienapfel* berufend, ihm folgend *Birklbauer/Hilf/Tipold*[232] und sich ihnen anschließend *Komenda/Madl*[233] sind der Auffassung, dass sowohl das Vermögen als auch das Interesse an der Verfügbarkeit und am Fortbestand von Daten durch § 126a geschützt ist.[234] Nach *Reindl-Krauskopf* wird von § 126a ausschließlich das Vermögen als Rechtsgut geschützt.[235] Im Ergebnis gleichen sich diese Meinungen, sodass auch das Affektionsinteresse vom Schutzbereich des § 126a erfasst wird.

---

221 JAB 359 BlgNR XVII. GP, 17; vgl dazu *Bertel* in Höpfel/Ratz (Hrsg), Wiener Kommentar zum Strafgesetzbuch[2] § 126a Rz 9 (Stand Dezember 2008); *Bergauer/Schmölzer*, Strafrecht, in Jahnel/Mader/Staudegger (Hrsg), IT-Recht[3] (2012) 635 (648); *Fabrizy*, Strafgesetzbuch StGB samt ausgewählten Nebengesetzen: Kurzkommentar[11] (2013) § 126a Rz 1.

222 *Reindl-Krauskopf*, Computerstrafrecht[2], 3; *Fuchs/Reindl-Krauskopf*, Strafrecht – Besonderer Teil I: Delikte gegen den Einzelnen[4] (2014) 139.

223 Übereinkommen über Computerkriminalität des Europarates, ETS 185; Die Ratifikation erfolgte erst 2012 durch BGBl III 140/2012; ausführlich dazu *Bergauer*, Gesetzgebungsmonitor Computerstrafrecht: Ratifikation des Übereinkommens über Computerkriminalität, jusIT 2012/95, 205 (205 f).

224 Rahmenbeschluss 2005/222/JI des Rates vom 24.2.2005 zum Schutz von Informationssystemen, ABl L 2005/69.

225 ErlRV 1166 BlgNR XXI. GP, 27; ErlRV 285 BlgNR XXIII. GP, 3 f; *Komenda/Madl* in SbgK § 126a Rz 5 ff.

226 BGBl 605/1987.

227 *Komenda/Madl* in SbgK § 126a Rz 4.

228 Strafrechtsänderungsgesetz 2008, BGBl I 109/2007.

229 ErlRV 285 BlgNR XXIII. GP, 8.

230 Vgl dazu *Sonntag*, Die EU-Richtlinie über Angriffe auf Informationssysteme, jusIT 2014/2, 8 (9).

231 *Kienapfel*, Grundriß des österreichischen Strafrechts – Besonderer Teil II[3] (1993) § 126a Rz 5.

232 *Birklbauer/Hilf/Tipold*, Strafrecht – Besonderer Teil I[2] (2012) § 126a Rz 1.

233 *Komenda/Madl* in SbgK § 126a Rz 17.

234 *Komenda/Madl* in SbgK § 126a Rz 15 ff.

235 *Reindl-Krauskopf*, Computerstrafrecht[2], 20 f.

5.2.1.3. Deliktstyp

§ 126a ist ein Erfolgsdelikt,[236] da zur Erfüllung des objektiven Tatbestandes der „Eintritt einer von der Tathandlung zumindest gedanklich abtrennbaren Wirkung in der Außenwelt“ in der Form eines tatbildlichen Schadens vorausgesetzt wird.[237] Ferner liegt ein Vorsatz-, Allgemein-, und Offizialdelikt vor. Aufgrund der rechtlichen Gleichwertigkeit der Tathandlungen ist § 126a ein alternatives Mischdelikt.[238] Die Ausgestaltung des Delikts als alternatives Mischdelikt hat zur Konsequenz, dass aus strafprozessualer Sicht keine Beschwer vorliegt, wenn das Gericht die Tat unter die falsche Tatbegehungsvariante subsumiert.[239] Das Delikt der Datenbeschädigung kann hinsichtlich der Tatbegehungsform des Unterdrückens als Dauerdelikt auftreten.[240] Zudem ist § 126a ein Beschädigungsdelikt, weil Daten als besondere Vermögenswerte vor Beeinträchtigungen geschützt werden.[241] Dieses Delikt kann auch als unechtes Unterlassungsdelikt auftreten.[242]

5.2.2. Objektiver Tatbestand

5.2.2.1. Tatsubjekt

Als Täter kommt in Betracht, wer Daten beschädigt, über die er nicht oder nicht allein verfügungsberechtigt ist.[243] Alleine verfügungsberechtigt iSd § 126a ist grundsätzlich derjenige, der Daten in den Computer eingibt und abspeichert.[244] Wird die Datenerstellung beauftragt, kommt dem Auftraggeber das alleinige Verfügungsrecht zu.[245] Nach *Reindl-Krauskopf* hat der Alleinverfügungsbefugte eine eigentümerähnliche Stellung und kann daher „seine“ Daten straflos löschen oder nach Belieben verändern.[246]

Als Täter kommt hingegen derjenige in Betracht, der nicht alleine über die Daten verfügen darf. Bspw kann sich ein Mitglied eines Programmierer-Teams strafbar machen, wenn er den Quellcode einer Website ohne die vorherige Zustimmung der anderen Entwickler löscht.[247] Die Verfügungsberechtigung ist sowohl übertragbar als auch beschränkbar, sodass nur bestimmte Daten genutzt oder auf eine bestimmte Weise verändert werden dürfen (zB ein Arbeitnehmer

---

[236] *Komenda/Madl* in SbgK § 126a Rz 12; vgl auch *Wessely*, Datenbeschädigung, in Mitgutsch/Wessely (Hrsg), Handbuch Strafrecht: Besonderer Teil I (2013) 234 (234).
[237] *Kienapfel/Höpfel/Kert*, Grundriss des Strafrechts Allgemeiner Teil[14] (2012) Z 9 Rz 6 f.
[238] *Bergauer/Schmölzer* in Jahnel/Mader/Staudegger, IT-Recht[3], 635 (648).
[239] *Komenda/Madl* in SbgK § 126a Rz 11.
[240] *Komenda/Madl* in SbgK § 126a Rz 13.
[241] *Komenda/Madl* in SbgK § 126a Rz 14.
[242] *Komenda/Madl* in SbgK § 126a Rz 85.
[243] Vgl dazu *Bertel* in WK-StGB[2] § 126a Rz 2; *Komenda/Madl* in SbgK § 126a Rz 26.
[244] *Komenda/Madl* in SbgK § 126a Rz 28.
[245] *Reindl-Krauskopf*, Computerstrafrecht[2], 19.
[246] Siehe *Reindl-Krauskopf*, Computerstrafrecht[2], 19.
[247] *Komenda/Madl* in SbgK § 126a Rz 30.

mit beschränkten Zugriffsrechten auf bestimmte Dateiordner).[248] Die Reichweite der Berechtigung wird im Regelfall von Vereinbarungen abhängen und ist stets im Einzelfall festzustellen.[249]

5.2.2.2. Tatobjekt

Tat- bzw Angriffsobjekt des § 126a sind „automationsunterstützt verarbeitete, übermittelte oder überlassene Daten, über die der Täter nicht oder nicht alleine verfügen darf".[250] Zur Klärung des Begriffes „automationsunterstützt verarbeitete, übermittelte oder überlassene Daten" sind die einschlägigen Bestimmungen des DSG 2000[251] heranzuziehen.[252] Nach § 4 Z 9 DSG 2000 ist unter automationsunterstützter Datenverarbeitung das elektronische Erfassen, Speichern, Ordnen, Vergleichen, Verändern, Verknüpfen, Vervielfältigen, Ausgeben oder Löschen von Daten zu verstehen. Nach § 4 Z 11 und 12 DSG 2000 gelten Daten als überlassen oder übermittelt, wenn sie an jemanden weitergegeben werden.

Der strafrechtliche Datenbegriff war zunächst in § 126a Abs 2 aF definiert und wurde mit dem StRÄG 2002 in § 74 Abs 2 verschoben, da eine Reihe neu eingeführter Computerstrafdelikte (zB §§ 118a, 119a, 126c) diesen Terminus verwendeten.[253] Der österreichische Gesetzgeber stellte im Unterschied zu Art 1 lit b CyCC lediglich klar, dass neben (direkt und indirekt) personenbezogenen Daten auch nicht personenbezogene Daten und Programme erfasst sind, ohne den Begriff „Daten" näher zu erläutern.[254] Im Vergleich zu den internationalen Vorgaben, welche unter dem Begriff „Daten" nur Computerdaten[255] verstehen, ist der österreichische Datenbegriff wesentlich weiter formuliert und erfasst sowohl digitale als auch analoge Daten (zB Bücher).[256]

Obwohl im StGB nicht ausdrücklich von Computerdaten die Rede ist, wird der strafrechtliche Datenbegriff zumeist in den Tatbeständen der Computerstrafdelikte (zB §§ 118a, 119a, 126a,

---

248 *Reindl-Krauskopf*, Computerstrafrecht[2], 19 f.
249 *Komenda/Madl* in SbgK § 126a Rz 26.
250 *Birklbauer/Hilf/Tipold*, BT I[2] § 126a Rz 4.
251 Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz 2000 – DSG 2000), BGBl I 165/1999 idF I 83/2013.
252 *Bertel* in WK-StGB[2] § 126a Rz 1; vgl dazu auch *Beer*, Convention on Cybercrime und österreichisches Strafrecht (2005) 144.
253 *Jerabek/Reindl-Krauskopf/Schroll* in Höpfel/Ratz (Hrsg), Wiener Kommentar zum Strafgesetzbuch[2] § 74 Rz 61 (Stand Juli 2013).
254 ErlRV 1166 BlgNR XXI. GP, 23; *Jerabek/Reindl-Krauskopf/Schroll* in WK-StGB[2] § 74 Rz 64; vgl dazu auch *Nittel* in Triffterer/Rosbaud/Hinterhofer (Hrsg), Salzburger Kommentar zum Strafgesetzbuch § 74 Rz 177 (Stand November 2006).
255 Computerdaten sind Darstellungen von Tatsachen, Informationen und Konzepten in einer für die Verarbeitung in einem Computersystem geeigneten Form einschließlich eines Programms, das die Ausführung einer Funktion durch ein Computersystem auslösen kann; vgl dazu Art 1 lit b CyCC; Art 1 lit b RB 2005/222/JI; Art 2 lit b RL 2013/40/EU.
256 *Komenda/Madl* in SbgK § 126a Rz 21.

126b, 148a) verwendet.[257] Diese Delikte setzen voraus, dass Daten entweder in digitaler bzw „computertechnisch bearbeitbarer Form“ vorliegen oder vom Täter mittels Eingabe in eine für die „unmittelbare automationsunterstützte (Weiter-)Verarbeitung“ geeignete Form gebracht werden.[258]

Computerprogramme sind nach *Jerabek/Reindl-Krauskopf/Schroll* als Daten iwS zu bezeichnen, weil „sie nicht primär der Darstellung von Aussagen, Tatsachen oder vergleichbaren Informationen dienen, sondern lediglich die Ausführung von Funktionen durch einen Computer auslösen“.[259] Nach *Komenda/Madl* ist die Unterscheidung zwischen Daten und Programmen nicht erforderlich, da Computerprogramme selbst aus Daten bestehen.[260]

5.2.2.3. Tathandlungen

Die Tatbegehungsformen des § 126a (Verändern, Löschen, Sonst-Unbrauchbarmachen und Unterdrücken) erfassen eine Vielzahl von Verhaltensweisen.[261] Unerheblich ist, ob die Tathandlung durch direktes Einwirken auf die Daten (zB Zerstörung eines bespielten USB-Sticks) oder unter Zuhilfenahme von „Hacking-Werkzeugen“ bzw Malware erfolgt.[262] Das bloße Kopieren der Daten von einem Datenträger ist unter keine der in § 126a angeführten Tathandlungen subsumierbar, weil Daten dadurch nicht beeinträchtigt werden.[263]

5.2.2.3.1. Verändern

Unter Datenveränderung ist die Herstellung eines neuen Dateninhaltes zu verstehen.[264] Daten werden verändert, wenn bspw bestehende Daten überschrieben oder partiell gelöscht werden (zB einzelne Kundendaten aus dem Kundenverzeichnis entfernen).[265] Darüber hinaus werden Daten auch durch die Schaffung neuer Verknüpfungen iSd § 126a verändert.[266] Mit dem Füllen eines bisher leeren Speicherplatzes (zB das Kopieren einer Datei auf einen leeren USB-Stick) ist diese oder eine andere Tatbegehungsform nicht verwirklicht, da im konkreten Fall keine bestehenden Daten in ihrer Grundstruktur beeinflusst oder beeinträchtigt werden.[267]

---

[257] *Jerabek/Reindl-Krauskopf/Schroll* in WK-StGB² § 74 Rz 65.
[258] *Jerabek/Reindl-Krauskopf/Schroll* in WK-StGB² § 74 Rz 65.
[259] *Jerabek/Reindl-Krauskopf/Schroll* in WK-StGB² § 74 Rz 66.
[260] *Komenda/Madl* in SbgK § 126a Rz 22.
[261] *Komenda/Madl* in SbgK § 126a Rz 39.
[262] Vgl dazu *Komenda/Madl* in SbgK § 126a Rz 40.
[263] *Komenda/Madl* in SbgK § 126a Rz 41.
[264] *Komenda/Madl* in SbgK § 126a Rz 42 ff; *Birklbauer/Hilf/Tipold*, BT I² § 126a Rz 6.
[265] Siehe *Beer*, Convention on Cybercrime, 145.
[266] *Komenda/Madl* in SbgK § 126a Rz 42.
[267] *Komenda/Madl* in SbgK § 126a Rz 44.

5.2.2.3.2. Löschen

Das Löschen von Daten entspricht dem Wesen nach der Zerstörung körperlicher Sachen iSd § 125.[268] Aufgrund der älteren Bestimmung des § 3 Z 11 DSG 1978 wurde zwischen physischem und logischem Löschen differenziert.[269] Physisches Löschen nach § 3 Z 11 lit a DSG 1978 bezeichnete „das Unkenntlichmachen von Daten in der Weise, dass eine Rekonstruktion nicht möglich ist". Das logische Löschen gem § 3 Z 11 lit b DSG 1978 erfasste hingegen „die Verhinderung des Zugriffs auf Daten durch programmtechnische Maßnahmen". Nach *Komenda/Madl* gelten Daten iSd § 126a als gelöscht, wenn diese „irreversibel unkenntlich gemacht wurden und damit verloren sind".[270] Die Tatbegehungsform des Löschens erfasst die Fälle des physischen Löschens von Daten iSd DSG 1978.

5.2.2.3.3. Unterdrücken

Daten werden unterdrückt, wenn sie dem Verfügungsberechtigten vorübergehend oder dauerhaft entzogen werden und der Berechtigte die Daten in diesem Zeitraum nicht benutzen kann.[271] Wurden Daten hingegen nur kurzfristig entzogen, liegt keine Datenunterdrückung iSd § 126a vor, sofern die Verfügungsbefugnis bei objektiver Betrachtung nicht eingeschränkt ist.[272]

Daten gelten als unterdrückt, wenn der Täter bspw Datenträger (zB USB-Stick) durch Wegnahme oder Verstecken physisch entzieht oder die Daten durch eine Softwaresperre (zB Ransomware) verschlüsselt.[273] Das Unterdrücken entspricht somit dem logischen Löschen iSd § 3 Z 11 lit a DSG 1978.[274]

5.2.2.3.4. Sonst Unbrauchbarmachen

Die Tatbegehungsvariante des Sonst-Unbrauchbarmachens von Daten erfüllt eine Art Auffangfunktion und erfasst Fälle, die nicht unter die übrigen Tathandlungen subsumiert werden können.[275] Daten sind iSd § 126a sonst unbrauchbar, wenn diese in ihrer Gebrauchsfähigkeit derart beeinträchtigt werden, dass ihr bestimmungsgemäßer Gebrauch nicht mehr möglich ist. Der Anwendungsbereich wird allerdings als gering eingestuft, da insb die Tatbegehungshandlung des Veränderns von Daten erfüllt ist.[276]

---

[268] *Komenda/Madl* in SbgK § 126a Rz 45.
[269] *Birklbauer/Hilf/Tipold*, BT I[2] § 126a Rz 7; *Komenda/Madl* in SbgK § 126a Rz 45.
[270] *Komenda/Madl* in SbgK § 126a Rz 45.
[271] *Komenda/Madl* in SbgK § 126a Rz 47.
[272] *Komenda/Madl* in SbgK § 126a Rz 47.
[273] *Komenda/Madl* in SbgK § 126a Rz 48; vgl auch *Fuchs/Reindl-Krauskopf*, Strafrecht BT I[4], 140.
[274] *Komenda/Madl* in SbgK § 126a Rz 45.
[275] *Reindl-Krauskopf*, Computerstrafrecht[2], 22; *Komenda/Madl* in SbgK § 126a Rz 46.
[276] *Komenda/Madl* in SbgK § 126a Rz 46.

5.2.2.4. Taterfolg

Die oben genannten Tathandlungen müssen zu einem nicht nur vorübergehenden Vermögensschaden beim Opfer führen.[277] Der Schaden ist nach dem Aufwand der Wiederherstellung bzw der Kosten der Wiederbeschaffung der beschädigten Daten zu bestimmen.[278] Muss etwa ein Datenträger (zB CD-ROM) gekauft oder ein kostenpflichtiges Download getätigt werden, besteht der Schaden im Kaufpreis.[279] Zur Schadensberechnung ist ausschließlich der durch die Beschädigung entstandene unmittelbare Schaden an den Daten heranzuziehen.[280] Mittelbare Schäden (zB Imageschäden, Produktionsausfälle), die durch eine Datenbeschädigung verursacht werden, bleiben außer Betracht.[281]

Der Eintritt eines in Geld bestimmbaren (objektiven) Vermögensschadens ist allerdings nicht zwingend erforderlich, weil auch die Beeinträchtigung des subjektiven Interesses an der Verfügbarkeit und am Fortbestand der Daten (Affektionsinteresse) einen Schaden iSd § 126a darstellt.[282] Bspw werden gespeicherte Baby- oder Urlaubsfotos, die keinen objektiv bestimmbaren Wert im Vermögen des Opfers haben, als Tatobjekte von § 126a geschützt.[283]

Kein tatbildlicher Schaden ist eingetreten, wenn die Daten ohne großen Aufwand wiederbeschafft oder wiederhergestellt werden können.[284] Die Bagatellgrenze ist nicht überschritten, sofern eine Sicherungskopie vorhanden ist, ein Computerprogramm kostenlos heruntergeladen werden kann oder die Daten nach einem Neustart des Rechners sofort wieder verfügbar sind.[285]

Weiters liegt kein Schaden iSd § 126a vor, wenn vonseiten des Berechtigten das subjektive Interesse an der Verfügbarkeit und am Fortbestand der Daten fehlt oder kein vernünftiger Mensch einen Aufwand tätigen würde, um diese wiederherzustellen („wertlose Daten“).[286]

---

277 *Komenda/Madl* in SbgK § 126a Rz 49.

278 Vgl dazu *Komenda/Madl* in SbgK § 126a Rz 50; *Reindl-Krauskopf*, Computerstrafrecht[2], 23; *Bertel* in WK-StGB[2] § 126a Rz 5.

279 *Bertel* in WK-StGB[2] § 126a Rz 5.

280 *Komenda/Madl* in SbgK § 126a Rz 53; *Reindl-Krauskopf*, Computerstrafrecht[2], 24.

281 JAB 359 BlgNR XVII. GP, 17; vgl dazu *Komenda/Madl* in SbgK § 126a Rz 53; *Bertel* in WK-StGB[2] § 126a Rz 5; *Fabrizy*, StGB[11] § 126a Rz 3; *Birklbauer/Hilf/Tipold*, BT I[2] § 126a Rz 11; *Schmölzer*, Das neue Computerstrafrecht (Strafrechtsänderungsgesetz 1987), EDVuR 1988 H 1, 20 (20).

282 *Komenda/Madl* in SbgK § 126a Rz 51; *Reindl-Krauskopf*, Computerstrafrecht[2], 21; *Bergauer*, Rache-Virus, in Hinterhofer/Schütz (Hrsg), Fallbuch Straf- und Strafprozessrecht (2015) 141 (144).

283 *Reindl-Krauskopf*, Computerstrafrecht[2], 21; *Wessely* in Mitgutsch/Wessely, Handbuch Strafrecht, 234 (234).

284 *Komenda/Madl* in SbgK § 126a Rz 54.

285 *Bergauer*, Viren, Würmer, Trojanische Pferde – Computerstrafrecht auf dem Prüfstand, in BMJ (Hrsg), 35. Ottensteiner Fortbildungsseminar aus Strafrecht und Kriminologie (2007) 27 (39); *Bertel* in WK-StGB[2] § 126a Rz 6; *Birklbauer/Hilf/Tipold*, BTI[2] § 126a Rz 10; *Komenda/Madl* in SbgK § 126a Rz 54.

286 *Reindl-Krauskopf*, Computerstrafrecht[2], 21; *Komenda/Madl* in SbgK § 126a Rz 55; *Bergauer/Schmölzer* in Jahnel/Mader/Staudegger, IT-Recht[3], 635 (648); *Kmetic*, Grundzüge des Computerstrafrechts (2014) 16.

5.2.3. Subjektiver Tatbestand

Zur Erfüllung des subjektiven Tatbestands reicht gem § 7 Abs 1 iVm § 5 Abs 1 2. HS dolus eventualis als schwächste Ausprägungsform des Vorsatzes aus.[287] Der Eventualvorsatz des Täters muss sich im Falle der Wertqualifikationen auf die Schadenshöhe erstrecken bzw hinsichtlich des zweiten Qualifikationsfalles auf die Begehung der Tat als Mitglied einer kriminellen Vereinigung gerichtet sein.[288]

5.2.4. Qualifikationen

5.2.4.1. Wertqualifikationen

§ 126a Abs 2 erfasst zunächst zwei Wertqualifikationen (3.000 bzw 50.000 Euro).[289] Wie bereits ausgeführt, ist zur Schadensberechnung lediglich der unmittelbare Schaden heranzuziehen. Übersteigt der vom Täter verursachte Schaden 3.000 Euro, ist er mit Freiheitsstrafe von bis zu zwei Jahren oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen. Wurde ein 50.000 Euro übersteigender Schaden herbeigeführt, ist der Täter mit Freiheitsstrafe von sechs Monaten bis zu fünf Jahren zu bestrafen.

5.2.4.2. Begehung der Tat als Mitglied einer kriminellen Vereinigung

Mit dem StRÄG 2008 in Umsetzung des Art 7 RB 2005/222/JI wurde ein zweiter Qualifikationsfall in § 126a Abs 2 eingefügt, der die Begehung der Tat als Mitglied einer kriminellen Vereinigung unter Strafe stellt.[290] Nach § 278 Abs 2 ist unter einer kriminellen Vereinigung ein auf längere Zeit angelegter Zusammenschluss von mehr als zwei Personen zu verstehen, „der darauf ausgerichtet ist, dass von einem oder mehreren Mitgliedern der Vereinigung ein oder mehrere Verbrechen, andere erhebliche Gewalttaten gegen Leib oder Leben, nicht nur geringfügige Sachbeschädigungen, Diebstähle oder Betrügereien“ sowie weitere in Abs 2 leg cit aufgezählten Delikte ausgeführt werden.[291]

Im konkreten Zusammenhang ist allerdings fraglich, ob das in der Aufzählung nicht angeführte Computerstrafdelikt der Datenbeschädigung (§ 126a) unter den Begriff „nicht nur geringfügige Sachbeschädigungen, Diebstähle oder Betrügereien“ subsumiert werden kann.[292] Aufgrund der in den Gesetzesmaterialien vertretenen Auffassung, dass eine weitgehende Ähnlichkeit

[287] *Komenda/Madl* in SbgK § 126a Rz 56.
[288] Vgl *Komenda/Madl* in SbgK § 126a Rz 57.
[289] *Komenda/Madl* in SbgK § 126a Rz 58.
[290] ErlRV 285 BlgNR XXIII. GP, 8.
[291] Vgl *Komenda/Madl* in SbgK § 126a Rz 59.
[292] *Triffterer* in Triffterer/Rosbaud/Hinterhofer, Salzburger Kommentar zum Strafgesetzbuch § 278 Rz 42 (Stand Februar 2001).

zur Sachbeschädigung bezüglich der äußeren Vorgehensweise und des Unwertes besteht,[293] ist nach *Triffterer* die Datenbeschädigung ein vereinigungsfähiges Delikt, obwohl § 126a nicht ausdrücklich im Katalog des § 278 Abs 2 angeführt wurde.[294] Seines Erachtens seien hohe wirtschaftliche Schäden, welche durch die Planung fortgesetzter Datenbeschädigungen herbeigeführt werden, angemessen zu berücksichtigen und bereits im Vorfeld zu bekämpfen. *Plöchl* bezweifelt hingegen die Möglichkeit der Einordnung des § 126a als vereinigungsfähiges Delikt.[295]

5.2.5. Besonderheiten

5.2.5.1. Vollendung und Versuch

Das Delikt der Datenbeschädigung ist mit dem Eintritt eines Vermögensschadens rechtlich vollendet.[296] Hat der Täter mit vollem Tatentschluss gehandelt und diesen durch eine Ausführungshandlung oder zumindest durch eine ausführungsnahe Handlung iSd § 15 Abs 2 betätigt, liegt ein strafbarer Versuch vor.[297] Der Rücktritt vom Versuch ist nach Maßgabe des § 16 möglich.[298] Tritt das Delikt der Datenbeschädigung als Dauerdelikt auf, ist § 126a mit dem Eintritt des tatbildlichen Schadens vollendet, tatsächlich beendet allerdings erst, wenn die Unterdrückungshandlung aufhört.[299]

Die Beurteilung, ob eine Handlung die geforderte Ausführungsnähe erreicht hat, ist einzelfallbezogen vorzunehmen.[300] Eine ausführungsnahe Handlung liegt bspw vor, wenn der Täter eine Datei mit dem Vorsatz ansteuert und auswählt, um diese zu löschen.[301] Eine Ausführungshandlung liegt vor, wenn der Täter durch die Eingabe des Löschen-Befehls einzelne Dateien von der Festplatte entfernt.[302]

5.2.5.2. Beteiligung

Aufgrund der Ausgestaltung des § 126a als Allgemeindelikt, ist die Beteiligung unter den Voraussetzungen des § 12 möglich.[303] Wer daher einen anderen zur Begehung einer Datenbeschädigung auffordert, ist gem §§ 12 2. Fall, 126a als Bestimmungstäter zu bestrafen.

---

293 JAB 359 BlgNR XVII. GP, 17.
294 *Triffterer* in SbgK § 278 Rz 42.
295 *Plöchl* in Höpfel/Ratz (Hrsg), Wiener Kommentar zum Strafgesetzbuch[2] § 278 Rz 22 (Stand Jänner 2014).
296 *Komenda/Madl* in SbgK § 126a Rz 79; *Kienapfel/Höpfel/Kert*, Strafrecht AT[14] Z 21 Rz 25.
297 *Kienapfel/Höpfel/Kert*, Strafrecht AT[14] Z 22 Rz 1 ff.
298 Vgl dazu *Kienapfel/Höpfel/Kert*, Strafrecht AT[14] Z 23 Rz 1 ff.
299 *Kienapfel/Höpfel/Kert*, Strafrecht AT[14] Z 9 Rz 29.
300 *Komenda/Madl* in SbgK § 126a Rz 79.
301 *Komenda/Madl* in SbgK § 126a Rz 81.
302 *Komenda/Madl* in SbgK § 126a Rz 82.
303 *Komenda/Madl* in SbgK § 126a Rz 84.

Derjenige, der den unmittelbaren Täter unterstützt, indem er ihm automatisierte Hacking-Tools (zB Brute-Force-Programme) für Angriffe zur Verfügung stellt, kommt als Beitragstäter gem § 12 3. Fall iVm 126a in Betracht. Werden Daten im Zuge von Cyber-Angriffen längere Zeit unterdrückt, ist die Beteiligung bis zur tatsächlichen Beendigung der Unterdrückungshandlung als Beitragstäter iSd §§ 12 3. Fall, 126a möglich.[304]

5.2.5.3. Privilegierungen, Strafaufhebung durch tätige Reue

Wurden Daten zum Nachteil eines Angehörigen beschädigt, ist die Tat gem § 166 privilegiert.[305] Von der Privilegierung werden sowohl das Grunddelikt als auch die Qualifikationen des § 126a Abs 2 erfasst.[306] Handeln außenstehende Personen zum Vorteil des Täters, sind diese nach § 166 Abs 2 ebenso privilegiert.[307] Als Konsequenzen, die sich aus der Anwendbarkeit des § 166 ergeben, sind die wesentliche Reduktion des Strafrahmens sowie die Transformation vom Offizial- zu einem Privatanklagedelikt anzuführen.[308]

§ 126a ist im Katalog der entwendungsfähigen Delikte nicht enthalten, weshalb nach *Komenda/Madl* die analoge Anwendung des § 141 sinnvoll erscheint, sofern der Täter eine Datenbeschädigung aus Unbesonnenheit begeht.[309] Folglich wird § 126a von einem Offizial- zu einem Ermächtigungsdelikt. Darüber hinaus wird der Strafrahmen gem § 141 Abs 1 reduziert. Der Täter ist demnach mit Freiheitsstrafe bis zu einem Monat oder mit Geldstrafe bis zu 60 Tagessätzen zu bestrafen. Wird die Tat zum Nachteil eines Angehörigen begangen, bleibt der Täter gem § 141 Abs 3 straffrei.

Das Delikt der Datenbeschädigung ist in der Aufzählung des § 167 Abs 1 angeführt und stellt somit ein reuefähiges Delikt dar. Die Möglichkeit der Strafaufhebung durch tätige Reue erstreckt sich auch auf sämtliche Qualifikationen des § 126a Abs 2.[310] § 167 Abs 2 verlangt zur Aufhebung der Strafbarkeit die rechtzeitige, vollständige und freiwillige („ohne hierzu gezwungen zu sein“) Wiedergutmachung des Schadens oder eine vertragliche Verpflichtung hierzu.[311]

---

304 Siehe *Kienapfel/Höpfel/Kert*, Strafrecht AT[14] E 5 Rz 21.
305 *Komenda/Madl* in SbgK § 126a Rz 86.
306 *Kirchbacher* in Höpfel/Ratz (Hrsg), Wiener Kommentar zum Strafgesetzbuch[2] § 166 Rz 7 (Stand Juli 2013).
307 *Kirchbacher* in WK-StGB[2] § 166 Rz 27.
308 *Komenda/Madl* in SbgK § 126a Rz 87; ausführlich dazu *Kirchbacher* in WK-StGB[2] § 166 Rz 33 ff.
309 *Komenda/Madl* in SbgK § 126a Rz 88.
310 *Komenda/Madl* in SbgK § 126a Rz 77.
311 Ausführlich dazu siehe *Kirchbacher* in Höpfel/Ratz (Hrsg), Wiener Kommentar zum Strafgesetzbuch[2] § 167 Rz 23 ff (Stand Juli 2013).

5.2.5.4. Abgrenzungen und Konkurrenzen

Werden im Zuge eines widerrechtlichen Zugriffs auf Computersysteme auch Daten beschädigt, können § 126a und § 118a in echter Konkurrenz zueinander stehen.[312]

Hat der Täter einen Datenträger iSd § 125 beschädigt bzw zerstört (zB Zertrümmerung eines mit Daten beschriebenen USB-Sticks), verwirklicht er – entsprechenden Vorsatz vorausgesetzt – sowohl § 126a als auch § 125 in echter Idealkonkurrenz.[313] Anders ist der Fall zu beurteilen, wenn der Täter die auf einer Festplatte gespeicherten Daten löscht, ohne dabei die Hardware zu zerstören. In solchen Fällen ist davon auszugehen, dass § 125 hinter das speziellere Delikt der Datenbeschädigung zurücktritt.[314]

Erfüllt der Täter sowohl § 126a als auch § 126b, tritt § 126b aufgrund der in § 126b Abs 1 genannten Subsidiaritätsklausel hinter das Delikt der Datenbeschädigung zurück.[315]

5.2.6. Anwendbarkeit des § 126a auf Defacements und Virtuelle Sit-Ins

5.2.6.1. Objektiver Tatbestand

5.2.6.1.1. Tatsubjekt

Hacker, die Webseiten im Rahmen von Defacements verunstalten, fehlt die Alleinverfügungsberechtigung hinsichtlich der betroffenen Daten. Dasselbe gilt auch für Protestteilnehmer, die sich an DDoS-Angriffen auf Web-Server beteiligen. Daher kann gesagt werden, dass die Feststellung der Alleinverfügungsbefugnis im Zusammenhang mit „hacktivistischen“ Aktionen keine besonderen Probleme aufwirft.

Im Hinblick auf Online-Sitzblockaden kommen Webseiten-Betreiber, Internet-Provider und auch User als Verfügungsberechtigte in Betracht.[316] Der Webseiten-Betreiber ist hinsichtlich der Webseitendaten idR als Alleinverfügungsberechtigter anzusehen. Bezüglich der Server-Software wird dem Provider im Regelfall eine alleinige Verfügungsbefugnis zukommen. Auch User kommen als Verfügungsberechtigte in Frage, bspw wenn Daten dauerhaft auf einem Server gespeichert werden (zB Cloud-Dienste).

---

312 *Komenda/Madl* in SbgK § 126a Rz 89.
313 *Komenda/Madl* in SbgK § 126a Rz 90; *Bertel* in WK-StGB² § 126a Rz 10; vgl auch *Bergauer/Schmölzer* in Jahnel/Mader/Staudegger, IT-Recht³, 635 (650).
314 *Bertel* in WK-StGB² § 126a Rz 9; *Komenda/Madl* in SbgK § 126a Rz 90.
315 *Komenda/Madl* in SbgK § 126a Rz 91; näheres dazu siehe 5.3.5.4.1.
316 *Wengenroth*, Zur Strafbarkeit Virtueller Sit-Ins: Zugleich ein Beitrag zur (Mit)Täterschaft bei minimalen Tatbeiträgen (2014) 50.

5.2.6.1.2. Tatobjekt

Tatobjekt des § 126a sind automationsunterstützt verarbeitete, übermittelte oder überlassene Daten. Im Rahmen politisch motivierter Defacements werden sichtbare Inhalte einer Webseite (zB Grafiken, Animationen, Texte udgl) verändert. Webseiten sind HTML-Dateien, die mithilfe von Computerprogrammen erstellt werden. Insofern fallen Webseiten unter den weit formulierten strafrechtlichen Datenbegriff des § 74 Abs 2 und sind folglich taugliche Tatobjekte des § 126a. Im Zuge von DDoS-Attacken werden regelmäßig Internetdienste (zB Web-Dienst) durch die Übermittlung unzähliger Datenpakete zum Absturz gebracht. Auch diese Server-Dienste (Programme iSd § 74 Abs 2) sind Tatobjekte des § 126a.

5.2.6.1.3. Tathandlungen

Als Tathandlungen kommen vielfältige Verhaltensweisen in Frage. Werden mithilfe einer SQL-Injection die in einer Datenbank gespeicherten Bilder bzw Texte einer Website durch politische Botschaften ersetzt, liegt die Tatbegehungsform des Veränderns vor, weil dadurch ein neuer Dateninhalt geschaffen wurde.[317] Es könnte auch die Tatbegehungsform des Löschens vorliegen, bspw wenn der Täter zusätzliche Inhalte entfernt und diese nicht mehr rekonstruiert werden können (zB Einträge in einem Forum). Wird im Zuge solcher Attacken etwa auch der Zugangscode geändert, sodass der Datenberechtigte nicht auf seine am Server gespeicherten Daten zugreifen kann, ist die Tathandlung des Unterdrückens verwirklicht. Aufgrund der Ausgestaltung des § 126a als alternatives Mischdelikt ist eine falsche Subsumtion aus strafprozessualer Sicht unerheblich.

Kommt es im Zuge von (D)DoS-Angriffen zu Ausfällen eines angegriffenen Servers, liegt nach *Bergauer* regelmäßig eine Datenunbrauchbarmachung bzw Datenunterdrückung iSd § 126a Abs 1 vor.[318] Ein nur kurzfristiger Entzug von Daten stellt allerdings kein Unterdrücken iSd § 126a dar, wenn der Berechtigte bei objektiver Betrachtung nicht eingeschränkt ist.[319] Nach *Wengenroth* ist eine Datenentziehung unter einer Stunde als kurzfristig anzusehen.[320] Können die Verfügungsberechtigten auch während einer Attacke auf die Daten zugreifen, liegt keine Datenunterdrückung vor. Die Tatbegehungsvarianten der Datenveränderung und Datenlöschung iSd § 126a sind im Falle virtueller Sit-Ins hingegen nicht einschlägig, da

[317] *Komenda/Madl* in SbgK § 126a Rz 42.
[318] *Bergauer*, Rezension zu Martin Daxecker in SbgK § 126b und § 126c. Auszug aus Triffterer/Rosbaud/Hinterhofer (Hrsg), Salzburger Kommentar zum StGB. LexisNexis Verlag. Wien, 26. Lfg (Mai 2012) EUR 39,00, jusIT 2012/93 (2012) 199 (200).
[319] *Komenda/Madl* in SbgK § 126a Rz 47.
[320] *Wengenroth*, Zur Strafbarkeit Virtueller Sit-Ins, 54.

bestehende Daten weder irreversibel unkenntlich gemacht noch neue Inhalte geschaffen werden.[321]

5.2.6.1.4. Taterfolg

Bei Web-Defacements kann ein objektiver Schaden bspw im Wiederherstellungsaufwand der Seiteninhalte erblickt werden (zB Bezahlung eines Web-Entwicklers). Sind Sicherungskopien vorhanden, die eine schnelle Wiederherstellung der veränderten Inhalte ermöglichen, liegt kein Schaden vor. Werden Web-Server im Zuge von DDoS-Angriffen lahmgelegt, kann dies durch einen Neustart des Rechners oder des Dienstes idR rasch behoben werden, weshalb in solchen Fällen kein unmittelbarer Schaden vorliegen wird. Mittelbare Schäden (zB Imageschäden) bleiben jedoch außer Betracht.[322] Zur Versuchsstrafbarkeit siehe 5.2.6.4.1.

5.2.6.2. Subjektiver Tatbestand

Zur Erfüllung des subjektiven Tatbestands genügt dolus eventualis. Dieses Erfordernis wird mE hinsichtlich virtueller Sit-Ins und Web-Defacements regelmäßig vorliegen.

5.2.6.3. Qualifikationen

5.2.6.3.1. Wertqualifikationen

Übersteigt der unmittelbare Schaden 3.000 bzw 50.000 Euro, ist der Täter gem § 126a Abs 2 nach den höheren Strafsätzen zu bestrafen. Fraglich ist, ob diese Wertgrenzen im Hinblick auf Web-Defacements oder virtuelle Sit-Ins überhaupt erreicht werden, da lediglich der unmittelbar aus der Datenbeschädigung resultierende Schaden maßgeblich ist. Sind etwa komplexe Webseiten von Defacements betroffen, kann der Wiederherstellungsaufwand uU die Wertgrenze von 3.000 Euro übersteigen. In Bezug auf Online-Sitzblockaden kann davon ausgegangen werden, dass diese Schwelle nicht erreicht wird.

5.2.6.3.2. Begehung der Tat als Mitglied einer kriminellen Vereinigung

Die Anwendbarkeit dieser Qualifikation ist dadurch eingeschränkt, dass § 126a in der Aufzählung des § 278 Abs 2 nicht enthalten ist. Werden Webseiten von einem Mitglied des Anonymous-Kollektivs verändert, ist die Bestrafung des Täters gem § 126a Abs 2 als Mitglied einer kriminellen Vereinigung nach *Triffterer*[323] möglich, sofern sämtliche weiteren objektiven und subjektiven Tatbestandsmerkmale des § 278 Abs 2 verwirklicht sind. Eine Strafbarkeit nach § 126a Abs 2 wird in Bezug auf virtuelle Sit-Ins jedoch regelmäßig am zeitlichen

[321] Vgl *Wengenroth*, Zur Strafbarkeit Virtueller Sit-Ins, 46.
[322] *Sonntag*, Einführung in das Internetrecht – Rechtsgrundlagen für Informatiker[2] (2014) 361.
[323] Vgl *Triffterer* in SbgK § 278 Rz 42.

Erfordernis („ein auf längere Zeit angelegter Zusammenschluss“) scheitern, bspw wenn Protestteilnehmer nach Aufrufen in sozialen Netzwerken (zB Twitter) spontan an derartigen Aktionen teilnehmen.[324]

5.2.6.4. Besonderheiten

5.2.6.4.1. Vollendung und Versuch

In Ermangelung eines tatbildlichen Schadens kommt sowohl bei Web-Defacements als auch bei virtuellen Sit-Ins die Strafbarkeit wegen versuchter Datenbeschädigung gem §§ 15, 126a in Betracht, sofern die Täter mit vollem Tatentschluss handeln und diesen zumindest durch eine ausführungsnahe Handlung iSd § 15 Abs 2 betätigen.[325]

Meines Erachtens gilt das Ansteuern der Sende-Taste im DDoS-Tool als ausführungsnahe Handlung. Sobald der Täter die Taste betätigt und damit Datenpakete zum Zweck der Datenunterdrückung an das Angriffsziel versendet, liegt eine Ausführungshandlung vor. Überwindet der Täter im Rahmen eines Web-Defacements eine Zugangssperre, indem er ein zuvor erlangtes Passwort verwendet, liegt eine ausführungsnahe Handlung vor, sofern der Täter mit dem Vorsatz handelt, die Inhalte der Webseiten durch politische Botschaften zu ersetzen.[326]

5.2.6.4.2. Beteiligung

Beitragstäter ist derjenige, der einen unmittelbaren Täter unterstützt, indem er zuvor Schwachstellen-Scans durchführt oder gespeicherte Passwörter in Web-CMS „knackt“, die in weiterer Folge vom Täter bei der Durchführung von Web-Defacements verwendet werden. Als Bestimmungstäter iSd §§ 12 2. Fall, 126a kommt in Betracht, wer einen anderen zur Durchführung von Web-Defacements beauftragt oder auffordert. Werden Daten während einer Online-Sitzblockade für längere Zeit unterdrückt, ist die Beteiligung nach § 12 3. Fall bis zur tatsächlichen Beendigung der Unterdrückungshandlung möglich.

5.2.6.4.3. Privilegierung und Strafaufhebung durch Tätige Reue

Die Anwendbarkeit des § 166 kommt im Falle „hacktivistischer“ Cyber-Angriffe nicht in Betracht, weil im Rahmen derartiger Cyber-Attacken keine Daten von Angehörigen beschädigt werden. Hingegen könnten politisch motivierte Angreifer tätige Reue iSd § 167 üben, indem

[324] *Öhlböck/Esztegar*, Rechtliche Qualifikation von Denial of Service Attacken, JSt 2011, 126 (131); vgl *Plöchl* in WK-StGB^2 § 278 Rz 8.
[325] *Kienapfel/Höpfel/Kert*, Strafrecht AT^{14} Z 22 Rz 6 ff.
[326] Vgl dazu *Komenda/Madl* in SbgK § 126a Rz 81.

sie den durch Web-Defacements oder virtuelle Sit-Ins verursachten Schaden freiwillig, rechtzeitig und vollständig wiedergutmachen, sofern ein solcher überhaupt vorliegt.

5.2.6.4.4. Abgrenzung und Konkurrenzen

Werden im Zuge von DDoS-Angriffen sowohl Daten unterdrückt bzw unbrauchbar gemacht als auch Computersysteme in ihrer Funktionsfähigkeit beeinträchtigt, tritt § 126b aufgrund der ausdrücklichen Subsidiaritätsklausel in § 126b Abs 1 hinter das Delikt der Datenbeschädigung zurück. Ausführlich zur Problematik siehe 5.3.5.4.1.

5.2.7. Ausblick

Nach den Materialien ist Art 5 RL 2013/40/EU bereits durch § 126a umgesetzt worden.[327] Eine Anpassung ist nur noch hinsichtlich der in Art 9 Abs 3 und 4 RL 2013/40/EU enthaltenen Qualifikationen erforderlich. Aus der Regierungsvorlage zum StRÄG 2015 geht hervor, dass nach § 126a Abs 2 die Herbeiführung eines 5.000 Euro übersteigenden Schadens mit Freiheitsstrafe bis zu 2 Jahren bedroht ist.[328]

In Umsetzung des Art 9 Abs 3 RL 2013/40/EU ist ein neuer Abs 3 vorgesehen.[329] Nach Abs 3 ist mit Freiheitsstrafe bis zu 3 Jahren zu bestrafen, „wer durch die Tat viele Computersysteme unter Verwendung eines Computerprogramms, eines Computerpassworts, Zugangscodes oder vergleichbarer Daten, die den Zugriff auf ein Computersystem oder einen Teil davon ermöglichen, sofern diese Mittel nach ihrer besonderen Beschaffenheit ersichtlich dafür geschaffen oder adaptiert wurden, beeinträchtigt“.[330] Anstatt der in Art 9 Abs 3 RL 2013/40/EU verwendeten Bezeichnung „beträchtliche Anzahl“ wird auf den Begriff „viele“ abgestellt, worunter ca 30 betroffene Computersysteme zu verstehen sind.[331]

In Umsetzung des Art 9 Abs 4 RL 2013/40/EU sind in § 126a Abs 4 weitere Qualifikationen enthalten.[332] Demnach ist mit Freiheitsstrafe von sechs Monaten bis zu fünf Jahren zu bestrafen, „wer durch die Tat einen 300.000 Euro übersteigenden Schaden herbeiführt (Z 1), durch die Tat wesentliche Bestandteile der kritischen Infrastruktur beeinträchtigt (Z 2), oder die Tat als Mitglied einer kriminellen Vereinigung begeht (Z 3)“.[333]

---

[327] Siehe ErlRV 689 BlgNR XXV. GP, 22.
[328] RV 689 BlgNR XXV. GP, 7.
[329] Vgl dazu ErlRV 689 BlgNR XXV. GP, 22.
[330] RV 689 BlgNR XXV. GP, 7.
[331] ErlRV 689 BlgNR XXV. GP, 22.
[332] ErlRV 689 BlgNR XXV. GP, 22.
[333] RV 689 BlgNR XXV. GP, 7.

Im Hinblick auf die häufige Verwendung des Begriffs „kritische Infrastruktur“ in den Qualifikationen der Computerstrafdelikte (§§ 118a, 126a und 126b) bzw der schweren Sachbeschädigung (§ 126 Abs 1 Z 5) soll § 74 Abs 1 Z 11 künftig eine entsprechende Definition enthalten.[334] Darunter sind Einrichtungen, Anlagen, Systeme oder Teile davon zu verstehen, „die eine wesentliche Bedeutung für die Aufrechterhaltung der öffentlichen Sicherheit und der Landesverteidigung, die Funktionsfähigkeit öffentlicher Informations- und Kommunikationstechnologie, die Verhütung oder Bekämpfung von Katastrophen, den öffentlichen Gesundheitsdienst, die öffentliche Versorgung mit Wasser, Energie sowie lebenswichtigen Gütern, des öffentlichen Abfallentsorgungs- und Kanalwesens oder den öffentlichen Verkehr haben“.[335]

Der Begriff „Informations- und Kommunikationstechnologie“ erfasst sämtliche Kommunikationsinstrumente bzw Anwendungen (zB Radio, Fernsehen, Hard- und Software für Computer, Rechnernetze, Mobiltelefone oder Satellitensysteme). Die Wendung „öffentlich“ ist iSv „der Allgemeinheit zugänglich bzw für diese bestimmt“ zu verstehen, obgleich der Staat oder ein Privater als Betreiber auftritt.[336]

5.3. Störung der Funktionsfähigkeit eines Computersystems[337]

5.3.1. Allgemeines

5.3.1.1. Hintergrund der Regelung und internationale Vorgaben

§ 126b wurde mit dem StRÄG 2002 als weiteres Computerstrafdelikt in das österreichische StGB eingeführt. Nach den Gesetzesmaterialien soll § 126b nur die Fälle der „reinen“ Dateneingabe bzw des „reinen“ Übermittelns von Daten erfassen, nicht aber die in Art 5 CyCC bzw Art 3 RB 2005/222/JI zusätzlich genannten Tathandlungen (Beschädigen, Löschen, Verändern, Beeinträchtigen oder Unterdrücken von Computerdaten).[338] Der österreichische Gesetzgeber geht davon aus, dass diese Handlungen zwingend zu einer Datenbeschädigung führen und daher von § 126a erfasst werden.[339]

Nach den Intentionen der Verfasser der CyCC soll Art 5 leg cit nur solche Angriffe auf Computersysteme (insb DoS-Attacken) pönalisieren, die ernste Auswirkungen für die Betreiber oder Eigentümer zur Folge haben, dh den Betrieb eines Systems verhindern oder

[334] ErlRV 689 BlgNR XXV. GP, 16.
[335] RV 689 BlgNR XXV. GP, 3.
[336] ErlRV 689 BlgNR XXV. GP, 16.
[337] § 126b idF BGBl I 109/2007.
[338] ErlRV 1166 BlgNR XXI. GP, 28; *Reindl-Krauskopf* in Höpfel/Ratz (Hrsg), Wiener Kommentar zum Strafgesetzbuch[2] § 126b Rz 4 (Stand Dezember 2008).
[339] ErlRV 1166 BlgNR XXI. GP, 28.

erheblich verlangsamen.[340] Insofern bietet auch § 126b keinen absoluten Schutz, weil lediglich schwere Störungen sanktioniert werden.[341] Die Zusendung unerwünschter E-Mails („Spam-Mails“) ist nicht gerichtlich strafbar, sofern es dadurch zu keinen schweren Funktionsstörungen eines Computersystems kommt.[342]

Mit dem StRÄG 2008 wurden in Umsetzung der Art 6 und 7 RB 2005/222/JI die in § 126b Abs 2 enthaltenen Qualifikationen geschaffen.[343] Inhaltliche Veränderungen waren nach der Auffassung des österreichischen Gesetzgebers hingegen nicht erforderlich. Art 4 RL 2013/40/EU enthält eine dem Art 5 RB 2005/222/JI entsprechende Regelung.[344]

5.3.1.2. Geschütztes Rechtsgut

Die Einordnung von § 126b in den sechsten Abschnitt des StGB verweist auf das Vermögen als schützenswertes Rechtsgut.[345] Dieses Computerstrafdelikt schützt die von schweren Funktionsstörungen freie Verwendungsmöglichkeit eines Systems als eigenständigen Vermögenswert.[346]

5.3.1.3. Deliktstyp

§ 126b ist ein Erfolgsdelikt, da über die Tathandlung hinaus der Eintritt einer schweren Störung der Funktionsfähigkeit des angegriffenen Computersystems zur Deliktsvollendung vorausgesetzt wird.[347] Aufgrund der Gleichwertigkeit der Tathandlungen ist § 126b ein alternatives Mischdelikt.[348] Zudem handelt es sich um ein Vorsatz- und Offizialdelikt.

5.3.2. Objektiver Tatbestand

5.3.2.1. Tatsubjekt

Unmittelbarer Täter des § 126b ist, wer die Funktionsfähigkeit eines Computersystems, über das er nicht oder nicht allein verfügen darf, durch die Eingabe oder Übermittlung von Daten schwer stört.[349] Nach *Reindl-Krauskopf* hat der Alleinverfügungsberechtigte eine eigentümerähnliche Stellung und kann wie der Eigentümer einer körperlichen Sache das

[340] Explanatory Report zur Convention on Cybercrime des Europarates Z 67; im Folgenden Explanatory Report.
[341] *Daxecker* in Triffterer/Rosbaud/Hinterhofer (Hrsg), Salzburger Kommentar zum Strafgesetzbuch § 126b Rz 12 (Stand Mai 2012).
[342] Vgl dazu Explanatory Report Z 69.
[343] *Daxecker* in SbgK § 126b Rz 10.
[344] *Sonntag*, jusIT 2014/2, 8 (9).
[345] *Daxecker* in SbgK § 126b Rz 11.
[346] *Reindl-Krauskopf* in WK-StGB^2 § 126b Rz 5.
[347] *Daxecker* in SbgK § 126b Rz 13; *Kienapfel/Höpfel/Kert*, Strafrecht AT^{14} Z 9 Rz 5 ff.
[348] *Daxecker* in SbgK § 126b Rz 14.
[349] *Daxecker* in SbgK § 126b Rz 19.

Computersystem nach Belieben zerstören oder zum Absturz bringen.[350] Das Eigentum an der Hardware ist jedoch nur ein Indiz für das Verfügungsrecht über das Gesamtsystem, denn ein PC kann auch zur eigenverantwortlichen Nutzung an eine andere Person überlassen werden.

Nach *Reindl-Krauskopf* ist ein mit umfassenden Verfügungsrechten ausgestatteter Arbeitnehmer (zB Systemadministrator) alleine verfügungsbefugt und kann einen Rechner straffrei zum Absturz bringen.[351] Sind hingegen andere Netzwerkrechner von der Störung betroffen, kann er sich trotzdem nach § 126b strafbar machen, wenn ihm die alleinige Verfügungsberechtigung hinsichtlich der anderen Rechner fehlt. Demgegenüber ist eine beschränkte Verfügungsbefugnis anzunehmen, wenn ein Nutzer keine Entscheidungsgewalt darüber hat, welche Programme er installieren bzw deinstallieren kann.[352] Die Verfügungsberechtigung ist stets einzelfallbezogen zu prüfen.

5.3.2.2. Tatobjekt

Tatobjekt des § 126b ist ein Computersystem, über das der Täter nicht oder nicht allein verfügen darf. Die Begriffsdefinition des Computersystems wurde mit dem StRÄG 2002 in das StGB aufgenommen und entspricht im Wesentlichen der Definition von Art 1 lit a CyCC.[353]

Ein Computersystem besteht gem § 74 Abs 1 Z 8 „sowohl aus einzelnen als auch verbundenen Vorrichtungen, die der automationsunterstützten Datenverarbeitung dienen“. Vorrichtungen sind zunächst sämtliche physischen Bauteile eines Rechners (zB Prozessor, Tastatur und Bildschirm).[354] Ein derartiges „Grundsystem“ ist durch zusätzliche Hardware-Komponenten erweiterbar, bspw durch eine angeschlossene Maus oder Drucker.[355] Unter den weiten strafrechtlichen Begriff „Computersystem“ fallen daher einzelne PCs sowie andere programmierbare Geräte (Mikrowellen, Waschmaschinen, Mobiltelefon udgl).[356]

Auch Computernetzwerke sind Computersysteme iSd § 74 Abs 1 Z 8, da es sich um den Zusammenschluss einzelner kleiner Systeme handelt. Auf die Art der Verbindung (zB kabelgebundene oder drahtlose Netze) sowie auf die Größe des Netzwerks (zB LAN, WAN) kommt es nicht an. Zur automationsunterstützten Datenverarbeitung werden neben der Hardware entsprechende System- bzw Programmdateien (zB Betriebssysteme) benötigt,

[350] *Reindl-Krauskopf* in WK-StGB^2 § 126b Rz 6.
[351] *Reindl-Krauskopf* in WK-StGB^2 § 126b Rz 8.
[352] *Reindl-Krauskopf* in WK-StGB^2 § 126b Rz 7.
[353] *Jerabek/Reindl-Krauskopf/Schroll* in WK-StGB^2 § 74 Rz 57.
[354] *Jerabek/Reindl-Krauskopf/Schroll* in WK-StGB^2 § 74 Rz 58.
[355] *Jerabek/Reindl-Krauskopf/Schroll* in WK-StGB^2 § 74 Rz 58.
[356] Vgl dazu *Nittel* in SbgK § 74 Rz 146; *Jerabek/Reindl-Krauskopf/Schroll* in WK-StGB^2 § 74 Rz 60; Explanatory Report Z 24.

weshalb auch unkörperliche Software-Komponenten als Vorrichtungen iSd § 74 Abs 1 Z 8 zu qualifizieren sind.[357]

5.3.2.3. Tathandlungen

§ 126b Abs 1 erfasst als Tathandlungen die Eingabe und Übermittlung von Daten.[358] Auf welche Weise die Daten eingegeben oder übermittelt werden ist unerheblich.[359] Als Handlungen iSd § 126b kommen daher die Dateneingabe mittels Maus oder Tastatur,[360] sowie auch das Versenden von Datenpaketen über aktive Internetverbindungen (zB E-Mails) in Betracht.[361]

5.3.2.4. Taterfolg

Zur Verwirklichung des Tatbestandes muss die Dateneingabe oder Datenübermittlung zu einer schweren Funktionsstörung eines Computersystems führen.[362] Die einschlägigen internationalen Vorgaben (CyCC und RB 2005/222/JI) geben keine Auskunft, ab welchem Ausmaß oder Zeitpunkt eine schwere Funktionsstörung angenommen werden kann.[363] Nach den Gesetzesmaterialien liegt eine schwere Störung iSd § 126b Abs 1 vor, wenn eine Attacke das Computersystem „völlig lahm legt oder etwa so verlangsamt, dass der verbleibende Gebrauchswert für den Betroffenen nicht wesentlich höher liegt als bei einem regelrechten Stillstand“.[364]

Im Unterschied zur Datenbeschädigung ist bei der Beurteilung des Schadens in erster Linie auf die tatbildliche schwere Störung eines Systems Bedacht zu nehmen.[365] Die Berücksichtigung von außertatbestandsmäßigen Schäden wird in den Gesetzesmaterialien nicht ausgeschlossen und kann bei der Strafzumessung eine Rolle spielen.[366] Bei schweren Störungen von Systemen ist zudem der zeitliche Aspekt im Zuge der strafrechtlichen Beurteilung zu beachten, da kurzfristige Ausfälle als nicht schützenswert angesehen werden.[367]

---

357 *Nittel* in SbgK § 74 Rz 145; *Jerabek/Reindl-Krauskopf/Schroll* in WK-StGB² § 74 Rz 59.
358 Vgl dazu *Fabrizy*, StGB¹¹ § 126b Rz 2.
359 *Reindl-Krauskopf* in WK-StGB² § 126b Rz 14.
360 *Beer*, Convention on Cybercrime, 155.
361 *Daxecker* in SbgK § 126b Rz 22.
362 *Fabrizy*, StGB¹¹ § 126b Rz 2.
363 *Reindl-Krauskopf* in WK-StGB² § 126b Rz 10.
364 ErlRV 1166 BlgNR XXI. GP, 29; vgl auch *Daxecker* in SbgK § 126b Rz 27.
365 *Daxecker* in SbgK § 126b Rz 28 ff.
366 Vgl dazu ErlRV 1166 BlgNR XXI. GP, 29; vgl auch *Fabrizy*, StGB¹¹ § 126b Rz 2.
367 ErlRV 1166 BlgNR XXI. GP, 29; *Bergauer* in BMJ, 35. Ottensteiner Fortbildungsseminar aus Strafrecht und Kriminologie, 27 (38); *Reindl-Krauskopf* in WK-StGB² § 126b Rz 9; vgl auch *Maleczky*, Das Strafrechtsänderungsgesetz 2002, JAP 2002/2003, 115 (115).

Nach *Reindl-Krauskopf* ist bei der Auslegung des objektiven Tatbestandsmerkmales „schwere Störung“ die Höhe des Wiederherstellungsaufwandes (zB Bezahlung eines Technikers) zu berücksichtigen, wobei nicht jeder Nachteil ausreicht.[368] Der finanzielle Aufwand muss ihres Erachtens die Wertgrenze von 1.000 Euro übersteigen. Der zeitliche Aspekt der Störung kann uU als ergänzendes Kriterium herangezogen werden, sofern sich der finanzielle Aufwand nicht bemessen lässt.[369]

Nach *Öhlböck/Esztegar* ist die Beurteilung der schweren Störung iSd § 126b Abs 1 „anhand eines beweglichen Systems mehrerer Kriterien“ vorzunehmen.[370] Als Beurteilungskriterien werden einerseits die faktischen Auswirkungen der Störung auf die Erreichbarkeit des Computersystems, das wirtschaftliche Ausmaß, und darüber hinaus die zeitliche Dauer des Wiederherstellungsaufwandes, nicht aber die Zeitdauer der Störungshandlung genannt.[371]

5.3.3. Subjektiver Tatbestand

Zur Erfüllung des subjektiven Tatbestandes genügt dolus eventualis.[372] Wird ein Computersystem ungewollt schwer gestört, ist diese Vorgehensweise gem § 7 Abs 1 straflos, da ein entsprechendes Fahrlässigkeitsdelikt fehlt.[373]

5.3.4. Qualifikationen

5.3.4.1. Längere Zeit andauernde Störung

Die Herbeiführung einer längeren Zeit andauernden Störung des Computersystems ist einem höheren Strafsatz unterworfen.[374] Anhaltspunkte, ab welcher Dauer eine derartige Störung vorliegt, kann aus dem Gesetz bzw den Materialien nicht entnommen werden.[375] Es ist aber darauf Bedacht zu nehmen, dass das zeitliche Kriterium bereits bei der Beurteilung schwerer Störungen gem § 126b Abs 1 berücksichtigt werden kann.[376] Nach *Reindl-Krauskopf* liegt eine tatbildliche Störung vor, wenn diese mehrere Tage andauert.[377]

Öhlböck/Esztegar sind hingegen der Ansicht, dass eine längere Zeit andauernde Störung iSd § 126b Abs 2 bereits ab einer Dauer von mehr als 24 Stunden anzunehmen ist, da schon

[368] *Reindl-Krauskopf* in WK-StGB² § 126b Rz 12; aA *Beer*, Convention on Cybercrime, 154.
[369] *Reindl-Krauskopf* in WK-StGB² § 126b Rz 13.
[370] *Öhlböck/Esztegar*, JSt 2011, 126 (128 f).
[371] *Öhlböck/Esztegar*, JSt 2011, 126 (129).
[372] *Birklbauer/Hilf/Tipold*, BT I² § 126b Rz 8; *Beer*, Convention on Cybercrime, 155.
[373] *Daxecker* in SbgK § 126b Rz 32.
[374] *Reindl-Krauskopf* in WK-StGB² § 126b Rz 18.
[375] ErlRV 285 BlgNR XXIII. GP, 8.
[376] ErlRV 285 BlgNR XXIII. GP, 8; vgl dazu auch ErlRV 1166 BlgNR XXI. GP, 29.
[377] *Reindl-Krauskopf* in WK-StGB² § 126b Rz 18.

mehrstündige Ausfälle spezieller Internetdienste (zB Online-Banking-Dienste) erhebliche Vermögensnachteile verursachen können.[378] Andererseits sind ihres Erachtens die meist sehr kurzen Reaktionszeiten im IT-Bereich zur Behebung dieser Störungen zu berücksichtigen.

Aufgrund der derzeit unklaren Kriterien hinsichtlich der Feststellung einer längeren Zeit andauernden Störung iSd § 126b Abs 2 sollte nach *Bergauer* auf ein dynamisches Beurteilungssystem abgestellt werden (zB zeitlicher Behebungsaufwand, Ausmaß der Störung).[379]

5.3.4.2. Begehung der Tat als Mitglied einer kriminellen Vereinigung

Nach § 126b Abs 2 ist die Begehung der Tat als Mitglied einer kriminellen Vereinigung mit Freiheitsstrafe von sechs Monaten bis zu fünf Jahren zu bestrafen. Der Begriff „kriminelle Vereinigung“ ist in § 278 Abs 2 definiert.[380] Das Delikt des § 126b ist nicht in der Aufzählung des § 278 Abs 2 enthalten und stellt somit kein vereinigungsfähiges Delikt dar. Im konkreten Zusammenhang reicht es zur Verwirklichung der Qualifikation des § 126b Abs 2 daher nicht aus, dass eine Vereinigung allein auf die Begehung des § 126b ausgerichtet ist.[381]

Nach *Reindl-Krauskopf* muss unabhängig davon eine kriminelle Vereinigung vorliegen.[382] Dieses Erfordernis ist etwa dann erfüllt, wenn ein auf längere Zeit angelegter Zusammenschluss von mehr als 2 Personen auf die Begehung eines der in § 278 Abs 2 genannten Delikte (zB Fälschung unbarer Zahlungsmittel iSd § 241a) ausgerichtet ist und diese Vereinigung bzw ein Mitglied eine schwere Funktionsstörung eines Computersystems herbeiführt.

5.3.5. Besonderheiten

5.3.5.1. Vollendung und Versuch

§ 126b ist mit Eintritt der schweren Funktionsstörung eines Computersystems (zB der Absturz eines Web-Dienstes) rechtlich vollendet.[383] Ist eine schwere Funktionsstörung nicht eingetreten, kommt eine Strafbarkeit wegen Versuchs gem §§ 15, 126b in Betracht. Die ausführungsnahe Handlung muss im Hinblick auf § 126c das Vorbereitungsstadium überschreiten. Eine ausführungsnahe Handlung iSd § 15 Abs 2 könnte vorliegen, wenn der

[378] *Öhlböck/Esztegar*, JSt 2011, 126 (129); zust *Daxecker* in SbgK § 126b Rz 34.
[379] *Bergauer* in Hinterhofer/Schütz, Fallbuch Straf- und Strafprozessrecht, 141 (148).
[380] Siehe dazu 5.2.4.2.
[381] *Daxecker* in SbgK § 126b Rz 35.
[382] *Reindl-Krauskopf* in WK-StGB^2 § 126b Rz 19.
[383] *Daxecker* in SbgK § 126b Rz 42.

Täter ein Schadprogramm (zB Computerwurm) an das Zielsystem versendet.[384] Der Rücktritt vom Versuch ist nach Maßgabe des § 16 möglich.[385]

5.3.5.2. Beteiligung

Die Beteiligung ist aufgrund der Konzeption des § 126b als Allgemeindelikt nach Maßgabe des § 12 möglich. Bspw kommt als Beitragstäter in Betracht, wer seinen Computer für DDoS-Angriffe zur Verfügung stellt. Beauftragt jemand einen anderen zur Versendung eines bösartigen Computerwurms, ist dieser als Bestimmungstäter zu qualifizieren.[386]

5.3.5.3. Privilegierung und Strafaufhebung durch Tätige Reue

Wird eine schwere Funktionsstörung des Computersystems eines Angehörigen herbeigeführt, ist die Tat gem § 166 privilegiert.[387] Weiters ist § 126b im Katalog des § 167 als reuefähiges Delikt angeführt. Im Übrigen kann auf die Ausführungen in 5.2.5.3 verwiesen werden.

5.3.5.4. Abgrenzungen und Konkurrenzen

5.3.5.4.1. Subsidiaritätsklausel

§ 126b ist aufgrund der in § 126b Abs 1 normierten Subsidiaritätsklausel zu § 126a subsidiär und tritt bei Verwirklichung beider Delikte hinter die Datenbeschädigung zurück.[388] Wird neben einer Datenbeschädigung iSd § 126a Abs 1 zugleich auch eine „längere Zeit andauernde Störung“ iSv § 126b Abs 2 bejaht, ist nach *Komenda/Madl* (unter Berufung auf die hL[389]) der Täter ausschließlich nach § 126a Abs 1 zu bestrafen, wenn der Schaden die Wertgrenzen des § 126a Abs 2 nicht übersteigt.[390]

Bergauer vertritt diesbezüglich die Auffassung, dass die Subsidiaritätsklausel aufgrund rechtspolitischer und teleologischer Erwägungen nur für schwere Funktionsstörungen iSd § 126b Abs 1 gelten kann, dh lediglich das Grunddelikt des § 126b hinter § 126a Abs 1 zurücktreten solle.[391] Im Übrigen ist der Anwendungsbereich des § 126b Abs 1 bereits dadurch eingeschränkt, dass § 126b hinter die versuchte Datenbeschädigung gem §§ 15, 126a zurücktritt.[392]

---

384 *Daxecker* in SbgK § 126b Rz 40.
385 *Daxecker* in SbgK § 126b Rz 41.
386 *Daxecker* in SbgK § 126b Rz 43.
387 *Daxecker* in SbgK § 126b Rz 39.
388 *Daxecker* in SbgK § 126b Rz 44; *Reindl-Krauskopf* in WK-StGB^2 § 126b Rz 20.
389 Vgl dazu *Birklbauer/Hilf/Tipold* BT I^2 § 126b Rz 1; *Daxecker* in SbgK § 126b Rz 44; *Reindl-Krauskopf* in WK-StGB^2 § 126b Rz 20.
390 *Komenda/Madl* in SbgK § 126a Rz 91.
391 *Bergauer*, jusIT 2012/93, 199 (200).
392 *Bergauer/Schmölzer* in Jahnel/Mader/Staudegger, IT-Recht^3, 635 (652).

5.3.5.4.2. Spam-Verbot

§ 107 Abs 2 TKG 2003[393] normiert das Verbot der unaufgeforderten Zusendung von E-Mails bzw SMS zum Zweck der Direktwerbung oder an mehr als 50 Empfänger, sofern diese nicht vorher eingewilligt haben.[394]

Verstöße gegen dieses Verbot sind gem § 109 Abs 3 Z 20 TKG 2003 Verwaltungsübertretungen, sofern dadurch keine schwere Funktionsstörung eines Computersystems iSd § 126b herbeigeführt wird. Kommt es durch den Versand von „Spam-Mails" zu schweren Störungen von Computersystemen (zB Absturz des SMTP-Servers), geht § 126b aufgrund der ausdrücklichen Anordnung in § 109 Abs 6 TKG 2003 der Verwaltungsstrafbestimmung vor.[395]

5.3.6. Anwendbarkeit des § 126b auf Web-Defacements und virtuelle Sit-Ins

5.3.6.1. Objektiver Tatbestand

5.3.6.1.1. Tatsubjekt

Als Täter kommt derjenige in Betracht, der durch Dateneingabe oder Datenübermittlung eine schwere Funktionsstörung eines Computersystems, über das er nicht oder nicht alleine verfügen darf, herbeiführt. Es ist davon auszugehen, dass einem politisch motivierten Angreifer jegliche Verfügungsbefugnis über das Zielsystem fehlen wird, weshalb er als Täter des § 126b in Frage kommt.

Im Zusammenhang mit virtuellen Sit-Ins ist zu bemerken, dass Rechner idR von tausenden Protestteilnehmern gleichzeitig angegriffen werden und diese mehrere Möglichkeiten zur Verfügung haben, sich an DDoS-Angriffen zu beteiligen.[396]

5.3.6.1.2. Tatobjekt

Online-Sitzblockaden verfolgen das primäre Ziel, bestimmte Serverdienste (zB E-Mail- oder Web-Dienst) zum Absturz zu bringen oder erhebliche Überlastungen herbeizuführen. In wenigen Fällen kann auch das Gesamtsystem abstürzen. Die Beurteilung des Tatobjekts ist auch dann unproblematisch, wenn im Zuge eines DDoS-Angriffs lediglich der Web-Dienst, nicht aber das gesamte System (Server) beeinträchtigt wird. Computerdienste stellen selbst

[393] Telekommunikationsgesetz 2003 (TKG 2003), BGBl I 70/2003 idF BGBl I 96/2013.
[394] *Daxecker* in SbgK § 126b Rz 45.
[395] Vgl dazu *Daxecker* in SbgK § 126b Rz 46.
[396] Ausführlich dazu 5.3.6.4.2.

Computersysteme dar, weil sie als Vorrichtungen iSd § 74 Abs 1 Z 8 der automationsunterstützten Datenverarbeitung dienen.[397]

5.3.6.1.3. Tathandlung

Im Falle virtueller Sit-Ins ist die Tatbegehungsvariante der Datenübermittlung verwirklicht,[398] da unter Zuhilfenahme von DDoS-Tools (zB LOIC) große Mengen von Datenpaketen (zB TCP-Pakete) über aktive Internetverbindungen an das Zielsystem versendet werden und dadurch den betroffenen Internetdienst erheblich überlasten oder zum Absturz bringen. Aufgrund der Konzeption des § 126b als alternatives Mischdelikt liegt aus strafprozessualer Sicht keine Beschwer vor, wenn die Handlung fälschlicherweise unter die Tatbegehungsform der Dateneingabe subsumiert wird.

5.3.6.1.4. Taterfolg

Die Tathandlungen müssen zu einer schweren Störung der Funktionsfähigkeit des Angriffszieles führen. Eine schwere Funktionsstörung iSd § 126b Abs 1 liegt jedenfalls vor, wenn der angegriffene Server bzw Web-Dienst abstürzt und auf Anfragen nicht mehr reagiert. Kurzfristige Ausfälle werden als nicht schützenswert angesehen, sodass mE ein Ausfall von mehr als einer Stunde eine schwere Störung iSd § 126b Abs 1 darstellt. Wird das angegriffene System hingegen kaum spürbar überlastet, liegt keine schwere Störung der Funktionsfähigkeit vor.

5.3.6.2. Subjektiver Tatbestand

Zur Verwirklichung des subjektiven Tatbestandes genügt dolus eventualis. Dieses Erfordernis wird im Hinblick auf politisch motivierte Cyber-Attacken idR erfüllt sein und bei der Beurteilung derartiger Sachverhalte keine Probleme bereiten.

5.3.6.3. Qualifikationen

5.3.6.3.1. Längere Zeit andauernde Störung

Aufgrund leistungsfähiger Server-Systeme ist mE nicht davon auszugehen, dass der erste Qualifikationsfall des § 126b im Hinblick auf virtuelle Sit-Ins verwirklicht wird. Kommt es dennoch zu schweren Funktionsstörungen über einen längeren Zeitraum, ist der Auffassung *Öhlböck/Esztegars* zu folgen, die eine längere Zeit andauernde schwere Störung bereits ab einer Dauer von mehr als 24 Stunden annehmen.[399]

---

[397] Vgl dazu *Bergauer*, jusIT 2012/93, 199 (200); *Bergauer/Schmölzer* in Jahnel/Mader/Staudegger, IT-Recht[3], 635 (650).
[398] *Wengenroth*, Zur Strafbarkeit Virtueller Sit-Ins, 65.
[399] *Öhlböck/Esztegar*, JSt 2011, 126 (129).

5.3.6.3.2. Begehung der Tat als Mitglied einer kriminellen Vereinigung

§ 126b ist nicht in der Aufzählung des § 278 Abs 2 als vereinigungsfähiges Delikt enthalten, weshalb die Anwendbarkeit dieser Qualifikation deutlich eingeschränkt ist.

Sofern das Hacktivisten-Kollektiv „Anonymous“ auf die Begehung eines der in § 278 Abs 2 genannten Straftaten gerichtet ist, bspw auf das Fälschen unbarer Zahlungsmittel gem § 241a, liegt bei Erfüllung sämtlicher anderer objektiver und subjektiver Tatbestandsmerkmale (insb der zeitlichen Komponente) eine kriminelle Vereinigung vor. Wird von Mitgliedern dieser Vereinigung ein DDoS-Angriff auf einen Web-Server durchgeführt und eine schwere Funktionsstörung herbeigeführt, ist die Anwendbarkeit des in Rede stehenden Qualifikationsfalles gegeben.

5.3.6.4. Besonderheiten

5.3.6.4.1. Vollendung und Versuch

§ 126b ist rechtlich vollendet, wenn eine schwere Funktionsstörung durch die Eingabe bzw Übermittlung von Daten verursacht worden ist. Im Zusammenhang mit virtuellen Sit-Ins ist der Fall denkbar, dass eine derartige Attacke nicht massiv genug ist, den „gegnerischen“ Web-Server zum Absturz zu bringen. Kommt es im Zuge eines DDoS-Angriffes zu keiner schweren Störung iSd § 126b Abs 1, liegt mE ein fehlgeschlagener und somit strafbarer Versuch vor, weil das Ziel, nämlich eine schwere Funktionsstörung herbeizuführen, höchstens durch einen neuerlichen Versuch erreicht werden kann.[400] Im konkreten Fall ist ein Rücktritt vom Versuch gem § 16 nicht möglich.

Bergauer wirft bezüglich der Teilnahme an virtuellen Sitzblockaden die Frage auf, ob die Handlung eines erst nach dem Absturz des Zielsystems hinzutretenden Ausführungstäters einen absolut untauglichen Versuch aufgrund eines untauglichen Tatobjekts darstellt.[401]

5.3.6.4.2. Beteiligung

An politisch motivierten DDoS-Angriffen nehmen idR tausende bzw zehntausende InternetnutzerInnen teil. Als Bereitstellende werden diejenigen Akteure bezeichnet, die ihre Rechner freiwillig zur Verfügung stellen. Befehlende sind Personen, welche die zuvor in freiwilligen Botnetzen verbundenen PCs aktivieren und diese während der Attacke fernsteuern. Beteiligen sich die Protestteilnehmer hingegen selbst am Angriff, indem sie durch

[400] *Kienapfel/Höpfel/Kert*, Strafrecht AT[14] Z 23 Rz 20 f.
[401] *Bergauer*, Rezension zu Lenard Wengenroth, Zur Strafbarkeit von virtuellen Sit-Ins. Zugleich ein Beitrag zur (Mit)Täterschaft bei minimalen Tatbeiträgen, jusIT 2014/116, 240 (240).

einen einzigen Mausklick im DDoS-Tool (zB LOIC) unzählige Datenpakete an das Angriffsziel übermitteln, werden sie als Angreifer bezeichnet.[402]

Angreifer bzw Befehlende gelten mE als unmittelbare Mittäter iSd § 12 1. Fall, da sie eine dem § 126b entsprechende Ausführungshandlung vornehmen, um das Angriffsziel mit Datenpaketen zu überfluten.[403] In Abgrenzung zum unmittelbaren Mittäter sind diejenigen Protestteilnehmer als Beitragstäter iSd § 12 3. Fall zu qualifizieren, die ihre Rechner für verteilte DoS-Angriffe einem freiwilligen Botnetz zur Verfügung stellen. Im Unterschied zum unmittelbaren Täter ist insb eine zeitliche Nähe zur Tat sowie eine deliktsspezifische Ausführungshandlung keine Voraussetzung für die Strafbarkeit.[404]

5.3.6.4.3. Abgrenzung und Konkurrenzen

Wird im Zuge eines DDoS-Angriffs die Funktionsfähigkeit des Zielsystems iSd § 126b beeinträchtigt, tritt § 126b aufgrund der ausdrücklichen Anordnung des § 126b Abs 1 hinter § 126a zurück, wenn dadurch auch Daten iSd § 126a unterdrückt werden. Aufgrund dieser Subsidiaritätsklausel tritt auch das vollendete Grunddelikt des § 126b hinter eine versuchte Datenbeschädigung gem §§ 15, 126a zurück.[405] Unter der Annahme, dass durch einen virtuellen Sit-In eine längere Zeit andauernde schwere Störung iSd §126b Abs 2 vorliegt und zugleich auch eine Datenbeschädigung iSd § 126a Abs 1 verwirklicht ist, sollte nach *Bergauer* ausschließlich das Grunddelikt des § 126b hinter § 126a Abs 1 zurücktreten.[406] Diesbezüglich wäre die Anwendbarkeit des § 126b Abs 2 gegeben.

Werden im Zuge von Online-Protesten eine Vielzahl unaufgeforderter Mails an mehr als 50 Personen versendet, liegt ein Verstoß gegen das in § 107 Abs 2 TKG 2003 normierte Verbot der unaufgeforderten Zusendung von E-Mails vor. Sofern dadurch keine schwere Funktionsstörung eines Computersystems auftritt, stellt die Tat eine Verwaltungsübertretung nach § 109 Abs 3 Z 20 TKG 2003 dar. Kommt es diesbezüglich jedoch zu schweren Störungen eines Mail-Servers, geht § 126b der Verwaltungsstrafbestimmung vor.

5.3.7. Ausblick

Art 4 RL 2013/40/EU ist nach den Gesetzesmaterialien bereits durch § 126b umgesetzt, weshalb ein Anpassungsbedarf lediglich in Bezug auf die Qualifikationen besteht.[407] Nach

---

402 *Wengenroth*, Zur Strafbarkeit virtueller Sit-Ins, 26.
403 Vgl *Kienapfel/Höpfel/Kert*, Strafrecht AT[14] E 3 Rz 3.
404 *Kienapfel/Höpfel/Kert*, Strafrecht AT[14] E 3 Rz 7 ff.
405 *Bergauer/Schmölzer* in Jahnel/Mader/Staudegger, IT-Recht[3], 635 (652).
406 *Bergauer*, jusIT 2012/93, 199 (200).
407 Vgl dazu ErlRV 689 BlgNR XXV. GP, 22.

Abs 2 ist mit Freiheitsstrafe bis zu zwei Jahren zu bestrafen, „wer durch die Tat eine längere Zeit andauernde Störung der Funktionsfähigkeit eines Computersystems herbeiführt".[408]

Wie auch bei § 126a soll im Zuge der Umsetzung des Art 9 Abs 3 RL 2013/40/EU ein neuer Abs 3 angefügt werden. Demnach ist zu bestrafen, „wer durch die Tat viele Computersysteme unter Verwendung eines Computerprogramms, eines Computerpassworts, Zugangscodes oder vergleichbarer Daten, die den Zugriff auf ein Computersystem oder einen Teil davon ermöglichen, sofern diese Mittel nach ihrer besonderen Beschaffenheit ersichtlich dafür geschaffen oder adaptiert wurden, schwer stört".[409] Die in § 126b Abs 4 vorgesehenen Qualifikationen gleichen jenen des § 126a Abs 4.[410]

5.4. Widerrechtlicher Zugriff auf ein Computersystem[411]

5.4.1. Allgemeines

5.4.1.1. Hintergrund der Regelung und internationale Vorgaben

§ 118a wurde mit dem StRÄG 2002 in das StGB eingefügt und stellt den widerrechtlichen Zugriff auf ein Computersystem unter Strafe.[412] Vor Inkrafttreten des § 118a war das bloße Eindringen in Computersysteme, sofern keine Daten iSd § 126a beschädigt wurden, straflos.[413]

Als internationale Vorschrift ist zunächst Art 2 CyCC zu beachten. Demnach soll jeder vorsätzliche und unbefugte Zugang zu einem Computersystem als Ganzes oder zu einem Teil davon unter Strafe gestellt werden. Die Vertragsstaaten der Konvention haben allerdings die Möglichkeit, sowohl den objektiven als auch den subjektiven Tatbestand entsprechend einzuschränken. Die Strafbarkeit kann nach Art 2 leg cit dadurch beschränkt werden, dass der Täter Sicherheitsmaßnahmen verletzt („by infringing security measures"), mit dem Vorsatz auf Datenspionage („with the intent of obtaining computer data") oder in einer anderen unredlichen Absicht handelt („other dishonest intent").[414]

Der österreichische Gesetzgeber hat von den angeführten Vorbehaltsmöglichkeiten Gebrauch gemacht. Einerseits wurde der objektive Tatbestand des § 118a dahingehend eingeschränkt,

---

[408] RV 689 BlgNR XXV. GP, 7.
[409] RV 689 BlgNR XXV. GP, 7.
[410] Siehe ErlRV 689 BlgNR XXV. GP, 22.
[411] § 118a idF BGBl I 109/2007.
[412] *Thiele* in Triffterer/Rosbaud/Hinterhofer (Hrsg), Salzburger Kommentar zum Strafgesetzbuch § 118a Rz 3 (Stand März 2007).
[413] Siehe *Reindl-Krauskopf* in Höpfel/Ratz (Hrsg), Wiener Kommentar zum Strafgesetzbuch[2] § 118a Rz 1 (Stand September 2008).
[414] Vgl dazu *Reindl-Krauskopf* in WK-StGB[2] § 118a Rz 2.

dass ein widerrechtlicher Zugriff nur dann vorliegt, wenn es zu einer Verletzung spezifischer Sicherheitsvorkehrungen kommt. Andererseits verlangt der subjektive Tatbestand neben dem Tatbildvorsatz in der Form des dolus eventualis einen komplexen erweiterten Vorsatz im Stärkegrad der Absicht.[415] Als weitere internationale Vorgabe ist Art 2 RB 2005/333/JI anzuführen. Die Umsetzung dieser Bestimmung erfolgte mit dem StRÄG 2008. Im Zuge dessen wurde der objektive Tatbestand hinsichtlich der Tathandlung erweitert, sodass bereits das Überwinden einer spezifischen Sicherheitsvorkehrung im System strafbar ist, und nicht wie bislang eine Verletzung von Sicherheitsmaßnahmen vorliegen musste.[416] Der subjektive Tatbestand wurde hingegen nicht verändert.

5.4.1.2. Geschütztes Rechtsgut

Durch die Einordnung des § 118a in den fünften Abschnitt des StGB verdeutlicht der Gesetzgeber, dass dieses Delikt die Privatsphäre als Rechtsgut schützt.[417] Das fremde Vermögen ist hingegen kein von § 118a geschütztes Rechtsgut.[418]

5.4.1.3. Deliktstyp

§ 118a ist ein Delikt mit überschießender Innentendenz, weil zusätzlich zum Tatbildvorsatz ein erweiterter Vorsatz in Form der Absichtlichkeit gefordert wird.[419] Darüber hinaus liegt ein Erfolgsdelikt vor, da sich der Täter Zugang zum System verschaffen muss, indem er eine spezifische Sicherheitsvorkehrung im System überwindet.[420] Nach *Wessely* ist § 118a als schlichtes Tätigkeitsdelikt zu qualifizieren.[421] Ferner ist § 118a ein Ermächtigungsdelikt.[422]

5.4.2. Objektiver Tatbestand

5.4.2.1. Tatsubjekt

Der Täter muss sich Zugriff zu einem Computersystem verschaffen, „über das er nicht oder nicht allein verfügen darf".[423] Hat jemand die Alleinverfügungsberechtigung über das gesamte System, kommt dieser nicht als Täter in Betracht.[424] Die Verfügungsbefugnis über das Computersystem erfüllt nach *Reindl-Krauskopf* eine ähnliche Aufgabe wie die Fremdheit der Sache bei § 125, weshalb der Berechtigte wie der Eigentümer einer körperlichen Sache über

---

415 *Reindl-Krauskopf* in WK-StGB² § 118a Rz 3.
416 *Reindl-Krauskopf* in WK-StGB² § 118a Rz 4.
417 *Thiele* in SbgK § 118a Rz 15.
418 *Thiele* in SbgK § 118a Rz 17.
419 *Thiele* in SbgK § 118a Rz 19.
420 *Thiele* in SbgK § 118a Rz 19.
421 *Wessely*, Widerrechtlicher Zugriff auf ein Computersystem, in Mitgutsch/Wessely (Hrsg), Handbuch Strafrecht: Besonderer Teil I (2013) 195 (196).
422 *Thiele* in SbgK § 118a Rz 19.
423 *Reindl-Krauskopf* in WK-StGB² § 118a Rz 10.
424 *Reindl-Krauskopf*, Computerstrafrecht², 12.

diese frei verfügen kann.[425] Die alleinige Verfügungsberechtigung kommt grundsätzlich demjenigen zu, der das System verwendet und gestaltet, bspw wenn er neue Hard- oder Software-Komponenten installiert.[426] Ist jemand bloß teilweise oder überhaupt nicht verfügungsberechtigt, kann er hingegen Täter sein.[427] Die Verfügungsbefugnis kann zudem an andere Personen übertragen (zB Systemadministrator mit umfassenden Zugriffsrechten) oder beschränkt werden.[428] Das Verfügungsrecht bezieht sich grundsätzlich nur auf das Computersystem, nicht aber auf die im System gespeicherten Daten, wobei diese Berechtigungen auch zusammenfallen können.[429].

5.4.2.2. Tatobjekt

Das Tatobjekt des § 118a ist ein Computersystem oder ein Teil eines solchen, über das der Täter nicht oder nicht allein verfügen darf.[430] Unter einem Computersystem sind nach § 74 Abs 1Z 8 einzelne oder verbundene Vorrichtungen zu verstehen, die der automationsunterstützten Datenverarbeitung dienen.[431]

5.4.2.3. Tathandlung und Erfolg

Die Tathandlung des § 118a verwirklicht, wer sich Zugriff zu einem Computersystem oder einem Teil davon verschafft, über das er nicht oder nicht allein verfügungsbefugt ist, indem er spezifische Sicherheitsvorkehrungen im System überwindet.[432]

5.4.2.3.1. Zugang-Verschaffen

Der Täter verschafft sich Zugang zum System, wenn er tatsächlich eindringt und innerhalb dieses Systems tätig werden kann.[433] Ein tatbildliches Eindringen liegt vor, wenn der Täter den physischen Zugang zu einem Rechner nutzt und unter Überwindung einer Sicherheitssperre in diesen „einsteigt“. Weiters verschafft sich der Täter Zugriff, wenn er über aktive Internetverbindungen das Computersystem penetriert.[434]

Die bloße Zugriffsmöglichkeit auf ein System entspricht hingegen nicht dem Tatbild des § 118a. Der Täter verschafft sich daher noch keinen Zugang, wenn er mithilfe des Ping-Befehls

---

425 *Reindl-Krauskopf*, Computerstrafrecht[2], 12 f.
426 *Reindl-Krauskopf*, Computerstrafrecht[2], 13.
427 *Thiele* in SbgK § 118a Rz 32.
428 *Reindl-Krauskopf*, Computerstrafrecht[2], 13.
429 *Reindl-Krauskopf*, Computerstrafrecht[2], 13.
430 *Thiele* in SbgK § 118 Rz 21.
431 Ausführlich dazu siehe 5.3.2.2.
432 *Reindl-Krauskopf* in WK-StGB[2] § 118a Rz 19.
433 Vgl dazu *Bergauer*, Phishing for nothing, in Hinterhofer/Schütz (Hrsg), Fallbuch Straf- und Strafprozessrecht (2015) 161 (171).
434 *Reindl-Krauskopf* in WK-StGB[2] § 118a Rz 20.

überprüft, ob der Zielrechner online ist. Dasselbe gilt für Port- oder Schwachstellen-Scans. In solchen Fällen verschafft sich der Täter erste nützliche Informationen über Schwächen in Computersystemen, ohne dabei in das „Systeminnere“ einzudringen.[435]

5.4.2.3.2. Überwinden spezifischer Sicherheitsvorkehrungen im System

§ 118a schützt nur gesicherte Computersysteme, weil der Täter zur Erfüllung des objektiven Tatbestandes eine spezifische Sicherheitsvorkehrung im System überwinden muss.[436] Nach den Gesetzesmaterialien sind Sicherheitsvorkehrungen spezifisch, „wenn sie im Computersystem angebracht worden sind, um sicherzustellen, dass nur berechtigte Personen auf das System zugreifen bzw unberechtigten Personen der Zugriff auf dieses System verwehrt wird“.[437]

Allgemeine Maßnahmen oder Vorrichtungen, die nicht im direkten Zusammenhang mit dem Computersystem stehen, bspw verschlossene Bürotüren, stellen keine spezifischen Sicherheitsvorkehrungen iSd § 118a dar.[438] Als Sicherungsmaßnahmen kommen sowohl Hardware-Module als auch Software-Komponenten (zB Passwortkontrollen, Hardware-Firewalls udgl) in Betracht.[439]

Nach *Reindl-Krauskopf* sind Sicherungen spezifisch, wenn „sie individuell gestaltet werden und geheim, also nur einem beschränkten Personenkreis bekannt sind bzw sein sollen“.[440] Ihres Erachtens erfüllen Standardpasswörter, die oftmals im Internet frei abrufbar sind, nicht die Erfordernisse einer spezifischen Sicherheitsvorkehrung iSd § 118a.[441] Sicherheitsmaßnahmen sind bspw nicht mehr geheim, sobald das Opfer dem Täter den Authentifizierungscode ausdrücklich mitteilt. Nach *Beer* ist diese Auffassung bedenklich, weil die Strafbarkeit dadurch erheblich eingeschränkt wird.[442] *Thiele* scheint hingegen keine besonderen Geheimhaltungstechniken zu verlangen.[443]

---

435 *Reindl-Krauskopf* in WK-StGB² § 118a Rz 21.
436 *Reindl-Krauskopf* in WK-StGB² § 118a Rz 22; *Fabrizy*, StGB¹¹ § 118a Rz 2; siehe auch *Kmetic*, Grundzüge des Computerstrafrechts, 13.
437 ErlRV 1166 BlgNR XXI. GP, 24.
438 *Reindl-Krauskopf* in WK-StGB² § 118a Rz 23; vgl auch ErlRV 1166 BlgNR XXI. GP, 24.
439 *Reindl-Krauskopf* in WK-StGB² § 118a Rz 23 f; vgl auch *Bergauer* in Hinterhofer/Schütz, Fallbuch Straf- und Strafprozessrecht, 161 (171).
440 *Reindl-Krauskopf*, Computerstrafrecht², 15.
441 *Reindl-Krauskopf*, Computerstrafrecht², 15 f; aA *Birklbauer/Hilf/Tipold*, Strafrecht BT² § 118a Rz 5.
442 *Beer*, Die Convention on Cybercrime, 121.
443 Vgl *Thiele* in SbgK § 118a Rz 39.

Vor dem StRÄG 2008 war zur Erfüllung des Tatbestandes die Verletzung einer spezifischen Sicherheitsvorrichtung iSd § 118a notwendig.[444] Eine tatbildliche Verletzung lag diesbezüglich vor, wenn eine Sicherung durch das Einwirken außer Kraft gesetzt oder nachteilig verändert bzw beeinträchtigt wurde, bspw durch das Deaktivieren der Antivirensoftware.[445] Seit dem StRÄG 2008 wird vom Täter nur noch ein Überwinden spezifischer Sicherheitsvorkehrungen gefordert.[446]

Nach *Reindl-Krauskopf* liegt ein tatbildliches Überwinden vor, sobald der Täter Anstrengungen unternimmt bzw es ihm Schwierigkeiten bereitet, in das Zielsystem einzudringen.[447] Wird bspw ein zuvor mittels Brute-Force-Attacke „geknacktes" Passwort zum Einstieg in das System verwendet, liegt ein Überwinden iSd § 118a vor.[448] Das Eindringen in Systeme unter Ausnutzung von Implementierungs- und Programmfehlern ist hingegen nicht tatbildlich iSd § 118a, sofern dadurch keine spezifischen Sicherheitssperren im System überwunden werden.[449] Verändert der Täter durch die Ausnutzung des Programmfehlers einen vom Benutzer eingerichteten Passwortschutz, ist ihres Erachtens eine im System angebrachte spezifische Sicherheitsvorrichtung überwunden.

5.4.3. Subjektiver Tatbestand

Der Tatbildvorsatz muss sich auf sämtliche objektive Tatbestandsmerkmale beziehen und zumindest im Stärkegrad des dolus eventualis vorliegen.[450] Zur Begründung der Strafbarkeit muss neben dem Tatbildvorsatz ein erweiterter Vorsatz des Täters in der Form der Absicht vorliegen.[451]

§ 118a Abs 1 verlangt zunächst die Absicht, „sich oder einem anderen Unbefugten von in einem Computersystem gespeicherten und nicht für ihn bestimmten Daten Kenntnis zu verschaffen" (Datenspionageabsicht).[452] Zur Auslegung des Begriffes „Daten" ist § 74 Abs 2 heranzuziehen.[453] Der erforderliche Vorsatz fehlt, wenn jemand aus Neugierde in ein System eindringt und seine technischen Fähigkeiten testet.[454] Darüber hinaus muss der Täter in der

---

444 *Reindl-Krauskopf*, Computerstrafrecht[2], 11.
445 *Bergauer*, Sniffer-Tools – unwillkommene Spyware, Ein Sniffer-Angriff unter § 118a StGB subsumiert, RdW 2006/391, 412 (414).
446 *Reindl-Krauskopf* in WK-StGB[2] § 118a Rz 26.
447 *Reindl-Krauskopf* in WK-StGB[2] § 118a Rz 26.
448 *Reindl-Krauskopf* in WK-StGB[2] § 118a Rz 27.
449 *Reindl-Krauskopf* in WK-StGB[2] § 118a Rz 29; aA *Sonntag*, Einführung in das Internetrecht[2], 352.
450 *Reindl-Krauskopf* in WK-StGB[2] § 118a Rz 34; *Thiele* in SbgK § 118a Rz 56.
451 Vgl *Reindl-Krauskopf* in WK-StGB[2] § 118a Rz 35; *Bergauer* in Hinterhofer/Schütz, Fallbuch Straf- und Strafprozessrecht, 161 (172); *Fabrizy*, StGB[11] § 118a Rz 3.
452 *Thiele* in SbgK § 118a Rz 60 ff.
453 Ausführlich dazu siehe 5.2.2.2.
454 *Reindl-Krauskopf* in WK-StGB[2] § 118a Rz 35.

Absicht handeln, die ausspionierten Daten entweder selbst zu benützen, einem andern Unbefugten weiterzuleiten oder zu veröffentlichen (Datenverwendungsabsicht).[455] Die tatsächliche Verwendung der Daten wird nicht gefordert.[456] Will der Täter die gespeicherten Daten bloß betrachten, fehlt die erforderliche Verwendungsabsicht. Weiters wird vom Täter die Absicht gefordert, „sich oder einem anderen einen Vermögensvorteil zuzuwenden oder einem anderen einen Nachteil zuzufügen“ (Gewinn- oder Schädigungsabsicht).[457]

Die Elemente des erweiterten Vorsatzes (dh Datenspionage-, Verwendungs- sowie Gewinn- oder Schädigungsabsicht) müssen im Zeitpunkt der Tathandlung vorliegen.[458] Das Eindringen in Computersysteme ist somit nicht strafbar, wenn sich der Täter erst zu einem späteren Zeitpunkt entschließt, die im System gespeicherten Daten auszuspionieren und in Gewinn- und Schädigungsabsicht zu verwenden.[459] Der subjektive Tatbestand des § 118a ist bspw nicht verwirklicht, wenn dem Täter zum Zeitpunkt der Errichtung von Botnetzen die erforderliche Spionageabsicht fehlt.[460]

5.4.4. Qualifikation

Die Tat ist gem § 118a Abs 3 mit Freiheitsstrafe bis zu drei Jahren bedroht, wenn der Täter als Mitglied einer kriminellen Vereinigung iSd § 278 Abs 2 handelt.[461] Diese Qualifikation wurde auf der Grundlage des Art 7 Abs 1 RB 2005/222/JI geschaffen,[462] welcher vorsieht, den unbefugten Zugang zu Informationssystemen mit einer Freiheitsstrafe von zwei bis fünf Jahren zu ahnden, wenn die Tat im Rahmen einer kriminellen Vereinigung begangen wird. Aus den Gesetzesmaterialien geht hervor, dass eine Freiheitsstrafe von drei Jahren als ausreichend erachtet wird.[463]

Wie im Fall der §§ 126a und 126b ist auch § 118a nicht im Katalog der vereinigungsfähigen Delikte des § 278 Abs 2 enthalten. Diesbezüglich kann es daher zu Anwendungsproblemen kommen, wenn die kriminelle Vereinigung ausschließlich auf die Begehung des § 118a ausgerichtet ist.[464]

---

455 *Thiele* in SbgK § 118a Rz 63 ff.
456 *Reindl-Krauskopf* in WK-StGB^2 § 118a Rz 36.
457 *Thiele* in SbgK § 118a Rz 67 ff.
458 *Reindl-Krauskopf* in WK-StGB^2 § 118a Rz 38.
459 *Thiele* in SbgK § 118a Rz 56.
460 Siehe dazu *Reindl-Krauskopf*, ÖJZ 2015/19, 112 (114).
461 *Reindl-Krauskopf* in WK-StGB^2 § 118a Rz 39.
462 ErlRV 285 BlgNR XXIII. GP, 7.
463 ErlRV 285 BlgNR XXIII. GP, 8.
464 Siehe 5.3.4.2.

5.4.5. Besonderheiten

5.4.5.1. Vollendung und Versuch

§ 118a ist rechtlich vollendet, sobald der Täter durch Überwindung einer spezifischen Sicherheitssperre tatsächlich in das Zielsystem gelangt.[465] Davor kann der Täter allenfalls wegen Versuchs strafbar sein. Ab welchem Zeitpunkt ein strafbarer Versuch gem §§ 15, 118a vorliegt, ist im Einzelfall zu beurteilen. Der Scan von Passwörtern mittels Brute-Force-Attacke ist nach *Reindl-Krauskopf* noch keine ausführungsnahe Handlung iSd § 15 Abs 2, weshalb der Täter straflos bleibt.[466] Ihres Erachtens liegt eine ausführungsnahe Handlung vor, wenn der Täter im Begriff ist, das zuvor erlangte Passwort für den Online-Einstieg in den Zielrechner zu nutzen. Eine Ausführungshandlung kann hingegen angenommen werden, wenn der Angreifer durch Passworteingabe in das System eindringt.[467] Port- und Schwachstellenscans sind zumindest hinsichtlich des unmittelbaren Täters als straflose Vorbereitungshandlungen zu qualifizieren.[468]

5.4.5.2. Beteiligung

Aufgrund der Konzeption des § 118a als Allgemeindelikt ist eine Beteiligung nach Maßgabe des § 12 möglich. Als Beitragstäter kommt derjenige in Betracht, der im Vorfeld einer Hacking-Attacke einen Port- oder Schwachstellenscan durchführt, sofern der unmittelbare Täter diese Ergebnisse verwendet und in das System eindringt. Nach *Thiele* ist Bestimmungstäterschaft gem §§ 12 2. Fall, 118a anzunehmen, wenn der Täter das Opfer als „willenloses Werkzeug" benutzt, indem er ein bösartiges Computerprogramm (zB Trojaner) durch das Opfer ausführen lässt, sodass Konfigurationen im System verändert und die gespeicherten Daten an den Täter versendet werden.[469]

5.4.5.3. Abgrenzung und Konkurrenzen

Werden im Zuge von Hacking-Attacken (zB Buffer-Overflows, SQL-Injection) keine spezifischen Sicherheitsvorkehrungen im System überwunden, ist der Täter nicht nach § 118a zu bestrafen.[470] Wurden jedoch gespeicherte Daten im Zusammenhang mit widerrechtlichen Zugriffen auf Computersysteme beschädigt, ist § 126a anwendbar. Werden Sicherheitssperren zugangskontrollgeschützter Dienste iSd § 10 ZuKG[471] (zB Pay-TV-Sendungen oder geschützte Online-Dienste) überwunden und verschafft sich der Täter

[465] *Reindl-Krauskopf* in WK-StGB² § 118a Rz 31.
[466] *Reindl-Krauskopf* in WK-StGB² § 118a Rz 30.
[467] *Reindl-Krauskopf* in WK-StGB² § 118a Rz 31.
[468] *Reindl-Krauskopf* in WK-StGB² § 118a Rz 32; *Thiele* in SbgK § 118a Rz 84.
[469] *Thiele* in SbgK § 118a Rz 86.
[470] *Thiele* in SbgK § 118a Rz 91.
[471] Bundesgesetz über den Schutz zugangskontrollierter Dienste (Zugangskontrollgesetz - ZuKG), BGBl I 60/2000 idF I 32/2001.

dadurch Zugang zu solchen Diensten, ist er ausschließlich nach § 10 ZuKG zu bestrafen, wenn er die Tat gem § 70 gewerbsmäßig ausgeführt hat.[472]

Nach § 10 Abs 3 ZuKG ist ein privater Nutzer derartiger Umgehungsvorrichtungen nicht strafbar.[473] Nach *Thiele* ist aufgrund der Verschiedenheit der Tathandlungen und Tatobjekte von § 118a und § 10 ZuKG keine Idealkonkurrenz zwischen den beiden Delikten anzunehmen.[474]

5.4.6. Anwendbarkeit des § 118a auf Web-Defacements und Virtuelle Sit-Ins

5.4.6.1. Objektiver Tatbestand

5.4.6.1.1. Tatsubjekt

Täter kann sein, wer sich Zugriff auf ein Computersystem oder einen Teil eines solchen verschafft, über das er nicht oder nicht alleine verfügen darf. Im Zusammenhang mit Web-Defacements kommt ein politisch motivierter Angreifer als Täter in Betracht, weil eine Alleinverfügungsbefugnis diesbezüglich nicht anzunehmen ist.

5.4.6.1.2. Tatobjekt

Das Tatobjekt des § 118a ist ein Computersystem iSv § 74 Abs 1 Z 8. Im Rahmen von Web-Defacements haben Angreifer die Möglichkeit, in Web-CMS einzudringen und die dort gespeicherten Webseiten-Inhalte zu verändern. Diese Programme dienen der automationsunterstützten Datenverarbeitung, dh der Erstellung oder Bearbeitung einer Webseite, und sind somit als Vorrichtungen iSd §74 Abs 1 Z 8 zu qualifizieren, die Teile eines Computersystems darstellen.

Eine weitere Möglichkeit, die sichtbaren Inhalte einer Webseite zu verunstalten besteht darin, mithilfe einer Code-Injection (zB SQL-Injection, XSS) Webseiten-Inhalte zu verändern, indem Schwachstellen in Web-Anwendungen ausgenutzt werden. Auch diese Anwendungen (zB Online-Shops) sind Teile eines Computersystems, da sie als Vorrichtungen der automationsunterstützten Datenverarbeitung dienen.

5.4.6.1.3. Tathandlung und Erfolg

Die Tathandlung ist verwirklicht, wenn sich der Täter unter Überwindung einer spezifischen Sicherheitsmaßnahme den Zugriff auf ein Computersystem verschafft, über das er nicht oder

[472] Vgl *Reindl-Krauskopf* in WK-StGB^2 § 118a Rz 41.
[473] *Thiele* in SbgK § 118a Rz 94.
[474] *Thiele* in SbgK § 118a Rz 95.

nicht alleine verfügungsberechtigt ist. Ob eine Handlung dem gesetzlichen Tatbild entspricht, ist einzelfallbezogen zu beurteilen.

Im Zusammenhang mit Web-Defacements ist je nach Angriffsmethode zu differenzieren. Werden bspw Webseiten verunstaltet, indem der Täter mithilfe einer Brute-Force-Attacke das Passwort eines Web-CMS „knackt", liegt eine Überwindung einer spezifischen Sicherheitsvorkehrung im System vor, sofern die Brute-Force-Attacke zielführend ist und der Angreifer in weiterer Folge in das System eindringt und tätig wird (zB Verändern oder Löschen von Inhalten einer Webseite).

Um Webseiten zu verunstalten, werden häufig Hacking-Techniken (zB SQL-Injections, XSS) eingesetzt, welche Schwachstellen in Web-Applikationen aufgrund von Programmierfehlern ausnutzen. Sind dadurch keine spezifischen Sicherheitsvorkehrungen im System (zB Passwortschutz oder Firewalls) überwunden worden, ist § 118a nicht anwendbar. Dies ist etwa der Fall, wenn ein Angreifer die in einer Datenbank gespeicherten Inhalte der Seite löschen oder verändern kann, ohne auf den Web-Server direkt zugreifen zu müssen. Dasselbe gilt, wenn im Zuge einer Social-Engineering-Attacke das Passwort dem Täter freiwillig mitgeteilt wird.

Mit der Durchführung von DDoS-Angriffen verfolgen die Akteure das primäre Ziel, Computersysteme (zB Web-Server) durch eine Vielzahl versendeter Anfragen erheblich zu überlasten bzw zum Absturz zu bringen. Es erfolgt somit kein widerrechtlicher Zugriff auf ein Computersystem, weshalb § 118a auf derartige Fälle nicht zur Anwendung kommt.[475]

5.4.6.2. Subjektiver Tatbestand

Bei Web-Defacements werden Webseiten-Inhalte verunstaltet. Zur Erfüllung des subjektiven Tatbestandes muss der Täter im Zeitpunkt der Tathandlung neben dem Tatbestandsvorsatz in der Absicht handeln, die im System gespeicherten Daten auszuspionieren und diese in Gewinn- oder Schädigungsabsicht zu verwenden.[476] Die Kriterien des erweiterten Vorsatzes sind in Bezug auf Web-Defacements mE jedoch nicht erfüllt. Verschafft sich der Täter nur deshalb Zugriff zu einem System, um die darin gespeicherten HTML-Dokumente iSd § 126a zu verändern oder zu löschen, fehlt dem Angreifer die erforderliche Verwendungsabsicht.[477]

---

[475] *Wengenroth*, Zur Strafbarkeit Virtueller Sit-Ins, 14.
[476] *Thiele* in SbgK § 118a Rz 58.
[477] Vgl dazu *Salimi*, Zahnloses Cyberstrafrecht? Eine Analyse der gerichtlichen Straftatbestände zum Daten- und Geheimnisschutz, ÖJZ 2012/115, 998 (999).

5.4.6.3. Qualifikation

Wie im Falle der §§ 126a und 126b ist auch § 118a nicht in der Aufzählung des § 278 Abs 2 als vereinigungsfähiges Delikt enthalten, weshalb die Anwendbarkeit in praxi deutlich eingeschränkt ist.

Unter der Annahme, dass ein Anonymous-Hacker als Mitglied einer kriminellen Vereinigung zu qualifizieren ist, und sämtliche objektiven bzw subjektiven Tatbestandselemente des § 118a erfüllt sind, muss diese Vereinigung allerdings auf die Begehung einer der in § 278 Abs 2 genannten Delikte gerichtet sein. Ist das nicht der Fall, kommt § 118a Abs 3 nicht zur Anwendung. Im Zusammenhang mit Web-Defacements wird aufgrund der fehlenden subjektiven Erfordernisse im Bereich des erweiterten Vorsatzes die Anwendbarkeit des § 118a Abs 3 ohnehin nicht gegeben sein.

5.4.6.4. Besonderheiten

5.4.6.4.1. Vollendung und Versuch

§ 118a ist vollendet, wenn sich ein Hacker den Zugriff zu einem System verschafft, indem er eine spezifische Sicherheitssperre (zB Passwortabfrage) umgeht. Hat der Täter noch keinen tatsächlichen Zugriff auf das Zielsystem, kann er wegen Versuchs strafbar sein. Die Brute-Force-Attacke selbst stellt allerdings noch keine ausführungsnahe Handlung iSd § 15 Abs 2 dar. Nach *Reindl-Krauskopf* liegt eine solche erst vor, wenn der Täter das zuvor erlangte Passwort einsetzen möchte. Das Scanning von Schwachstellen ist hinsichtlich des unmittelbaren Täters als straflose Vorbereitungshandlung zu qualifizieren.[478]

5.4.6.4.2. Beteiligung

Als Beitragstäter kommt bspw derjenige in Betracht, der seinen Computer zur Durchführung verteilter Brute-Force-Attacken zur Verfügung stellt. Weiters liegt Beitragstäterschaft gem §§ 12 3. Fall, 118a vor, wenn jemand einen Schwachstellen-Scan durchführt und damit das Eindringen in einen Server für den unmittelbaren Täter erleichtert oder ermöglicht. Als Bestimmungstäter gem §§ 12 2. Fall, 118a kommt in Frage, wer einen anderen beauftragt, in Web-Server einzudringen.

[478] *Reindl-Krauskopf* in WK-StGB^2 § 118a Rz 30.

5.4.6.4.3. Abgrenzung und Konkurrenzen

Aufgrund der eingeschränkten Anwendbarkeit des § 118a im Hinblick auf die Erfordernisse des subjektiven Tatbestandes ergeben sich hinsichtlich Web-Defacements daher keine Konkurrenzen. Allenfalls bleibt eine mögliche Strafbarkeit nach § 126a.

5.4.7. Ausblick

Mit dem StRÄG 2015 soll § 118a wie folgt geändert werden:[479]

> „§ 118a. (1) Wer sich zu einem Computersystem, über das er nicht oder nicht allein verfügen darf, oder zu einem Teil eines solchen durch Überwindung einer spezifischen Sicherheitsvorkehrung im Computersystem in der Absicht Zugang verschafft,
>
> 1. sich oder einem anderen Unbefugten Kenntnis von personenbezogenen Daten zu verschaffen, deren Kenntnis schutzwürdige Geheimhaltungsinteressen des Betroffenen verletzt, oder
> 2. durch die Verwendung von im System gespeicherten und nicht für ihn bestimmten Daten, deren Kenntnis er sich verschafft, einem anderen einen Nachteil zuzufügen,
>
> ist mit Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen.
>
> (2) Wer die Tat in Bezug auf ein Computersystem, das ein wesentlicher Bestandteil der kritischen Infrastruktur (§ 74 Abs. 1 Z 11) ist, begeht, ist mit Freiheitsstrafe bis zu zwei Jahren zu bestrafen.
>
> (3) Der Täter ist nur mit Ermächtigung des Verletzten zu verfolgen.
>
> (4) Wer die Tat nach Abs. 1 im Rahmen einer kriminellen Vereinigung begeht, ist mit Freiheitsstrafe bis zu zwei Jahren, wer die Tat nach Abs. 2 im Rahmen einer kriminellen Vereinigung begeht, mit Freiheitsstrafe bis zu drei Jahren zu bestrafen.“

Aus den Gesetzesmaterialien geht hervor, dass die bisherige Fassung des § 118a nicht alle Fälle des Phänomens „Hacking“ (insb die Einrichtung von Bot-Netzen) erfasst, weil Täter zumeist nicht in der Absicht handeln, Daten auszuspionieren. Im Zuge der Strafrechtsreform 2015 soll mit der Neufassung des § 118a eine Strafbarkeitslücke geschlossen werden.[480] Nach § 118a Abs 1 Z 1 ist zu bestrafen, „wer sich zu einem Computersystem […] in der Absicht Zugang verschafft, sich oder einem anderen Unbefugten Kenntnis von personenbezogenen Daten zu verschaffen, deren Kenntnis schutzwürdige Geheimhaltungsinteressen des Betroffenen verletzt“.

In § 118a Abs 1 Z 2 wird zukünftig das Phänomen „Bot-Netze“ erfasst.[481] Zur Klärung des in Abs 1 Z 2 leg cit benutzten Begriffes „Verwendung von […] Daten“ ist § 4 Z 8 DSG 2000 heranzuziehen.[482] Darunter ist „jede Art der Handhabung von Daten, also sowohl das Verarbeiten (Z 9) als auch das Übermitteln (Z 12) von Daten“ zu verstehen.

---

[479] RV 689 BlgNR XXV. GP, 6.
[480] ErlRV 689 BlgNR XXV. GP, 20.
[481] ErlRV 689 BlgNR XXV. GP, 21.
[482] ErlRV 689 BlgNR XXV. GP, 21.

Weiters ist in einem neuen Abs 2 eine Qualifikation vorgesehen, wonach der Täter mit Freiheitsstrafe bis zu zwei Jahren zu bestrafen ist, wenn er die Tat in Bezug auf ein Computersystem begeht, das einen wesentlichen Bestandteil der kritischen Infrastruktur darstellt.[483] Zudem ist die Begehung der Tat als Mitglied einer kriminellen Vereinigung nach Abs 4 mit höheren Strafsätzen bedroht.

5.5. Missbrauch von Computerprogrammen oder Zugangsdaten[484]

5.5.1. Allgemeines

5.5.1.1. Hintergrund der Regelung und internationale Vorgaben

§ 126c wurde mit dem StRÄG 2002 in Umsetzung der CyCC als spezielles Vorbereitungsdelikt in das StGB eingefügt, um insb die Herstellung und Verbreitung von Hacking-Tools unter Strafe zu stellen.[485] Im Zuge der Umsetzung des Art 6 CyCC hat der nationale Gesetzgeber von der Vorbehaltsmöglichkeit in Art 6 Abs 3 CyCC Gebrauch gemacht und den bloßen Besitz von Schadprogrammen, vergleichbaren Vorrichtungen und Zugangsdaten nicht unter Strafe gestellt, weil der Besitz von Programmen und Daten als Vorbereitungshandlungen „nicht die Schwelle erreicht, ab der eine Kriminalisierung gerechtfertigt erscheint".[486]

Mit dem StRÄG 2004[487] wurden die Tathandlungen des Sich-Verschaffens und der Besitz sowie das vorbereitende Delikt des § 148a nach Maßgabe des Rahmenbeschlusses 2001/413/JI zur Bekämpfung von Betrug und Fälschungen im Zusammenhang mit unbaren Zahlungsmitteln[488] in den objektiven Tatbestand des § 126c aufgenommen.[489]

5.5.1.2. Geschütztes Rechtsgut

Aufgrund der Einordnung dieser Strafbestimmung in den sechsten Abschnitt des StGB wird von § 126c vordergründig das Vermögen geschützt. Darüber hinaus werden vom Schutzbereich dieser Strafbestimmung auch die Rechtsgüter der in Abs 1 Z 1 leg cit genannten vorbereitenden Delikte erfasst.[490]

---

483 ErlRV 689 BlgNR XXV. GP, 21.
484 § 126c idF 15/2004.
485 *Bergauer/Schmölzer* in Jahnel/Mader/Staudegger, IT-Recht[3], 635 (654); *Reindl-Krauskopf* in Höpfel/Ratz (Hrsg), Wiener Kommentar zum Strafgesetzbuch[2] § 126c Rz 1 (Stand Dezember 2008); *Daxecker* in Triffterer/Rosbaud/Hinterhofer (Hrsg), Salzburger Kommentar zum Strafgesetzbuch § 126c Rz 1 (Stand Mai 2012).
486 *Reindl-Krauskopf* in WK-StGB[2] § 126c Rz 3; vgl auch ErlRV 1166 BlgNR XXI. GP, 29.
487 Strafrechtsänderungsgesetz 2004, BGBl I 15/2004.
488 Rahmenbeschluss 2001/413/JI des Rates vom 28.5.2001 zur Bekämpfung von Betrug und Fälschungen im Zusammenhang mit unbaren Zahlungsmittel, ABl L 2001/149.
489 *Daxecker* in SbgK § 126c Rz 7; vgl dazu ErlRV 309 XXII. GP, 7 f.
490 *Daxecker* in SbgK § 126c Rz 9.

5.5.1.3. Deliktstyp

§ 126c ist ein Vorbereitungsdelikt und pönalisiert Verhaltensweisen, die als Vorbereitungshandlungen straflos wären.[491] Ferner liegt ein Offizialdelikt vor, das aufgrund der Strafdrohung in die sachliche Zuständigkeit der Bezirksgerichte fällt. Nach *Daxecker* ist § 126c als schlichtes Tätigkeitsdelikt und kumulatives Mischdelikt zu qualifizieren.[492] Im Hinblick auf die Tatbegehungsvariante des Herstellens wird von *Bergauer* die Auffassung vertreten, dass § 126c Abs 1 ein Erfolgsdelikt darstellt.[493] § 126c ist als Vorsatzdelikt konzipiert und stellt im Besonderen ein Delikt mit überschießender Innentendenz dar, weil zur Erfüllung des subjektiven Tatbestandes ein erweiterter Vorsatz des Täters gefordert wird.[494] Nach *Bergauer* kann in § 126c ein abstraktes Gefährdungsdelikt erblickt werden, da zumeist nicht einmal der Täter die Gefährlichkeit hergestellter Schadprogramme (zB neuartige Computerwürmer) in Bezug auf Schaden und Reichweite abschätzen kann.[495] Im Gegensatz zu konkreten Gefährdungsdelikten reicht bereits die theoretische Möglichkeit der Beeinträchtigung von Tatobjekt bzw Rechtsgut zur Erfüllung des Tatbestandes aus.[496]

5.5.2. Objektiver Tatbestand

5.5.2.1. Tatsubjekt

Nach § 126c ist Täter, wer die in Abs 1 Z 1 leg cit genannten Tatmittel mit dem erweiterten Vorsatz herstellt, einführt, vertreibt, veräußert, sonst zugänglich macht, sich verschafft oder besitzt, dass diese zur Begehung der aufgezählten Delikte verwendet werden.

5.5.2.2. Beschränkung auf bestimmte Delikte

Als spezielles Vorbereitungsdelikt ist der Anwendungsbereich dieser Strafnorm auf die in § 126c Abs 1 Z 1 taxativ aufgezählten Delikte (§§ 118a, 119, 119a, 126a, 126b und 148a) beschränkt. *Bergauer* vertritt im konkreten Zusammenhang den Standpunkt, dass es aus kriminalpolitischen Gründen notwendig erscheint, das Delikt des Diebstahls (§ 127) als weitere Strafbestimmung in § 126c einzufügen, da nach Ansicht der Rsp die Geldbehebung mit einer

---

491 *Wessely*, Missbrauch von Computerprogrammen oder Zugangsdaten, in Mitgutsch/Wessely (Hrsg), Handbuch Strafrecht: Besonderer Teil I (2013) 239 (240); *Kienapfel/Höpfel/Kert*, Strafrecht AT^{14} Z 21 Rz 5 ff.

492 *Daxecker* in SbgK § 126c Rz 11; siehe dazu auch *Birklbauer/Hilf/Tipold*, BT I^{2} § 126c Rz 6; *Wessely* in Mitgutsch/Wessely, Handbuch Strafrecht, 239 (240).

493 *Bergauer* in Hinterhofer/Schütz, Fallbuch Straf- und Strafprozessrecht, 141 (150).

494 *Daxecker* in SbgK § 126c Rz 28.

495 *Bergauer*, Kritische Anmerkungen zu § 126c ÖJZ 2007/45, 532 (535); zust *Daxecker* in SbgK § 126c Rz 11; siehe auch *Birklbauer/Hilf/Tipold*, BT I^{2} § 126c Rz 4.

496 *Kienapfel/Höpfel/Kert*, Strafrecht AT^{14} Z 9 Rz 31 ff.

entfremdeten Bankomatkarte als Diebstahl iSd § 127 qualifiziert wird und somit das Ausspionieren des Zugangscodes von § 126c nicht erfasst wäre.[497]

5.5.2.3. Verpönte Tatmittel

5.5.2.3.1. Computerprogramme und vergleichbare Vorrichtungen

Computerprogramme und vergleichbare Vorrichtungen sind nach § 126c Abs 1 Z 1 nur dann als verpönte Tatmittel zu qualifizieren, wenn „sie nach ihrer besonderen Beschaffenheit ersichtlich zur Begehung der angeführten Straftaten geschaffen oder adaptiert wurden".[498] Unter vergleichbaren Vorrichtungen sind jene Mittel zu verstehen, die keine Computerprogramme darstellen, bspw Abhöranlagen oder Vorrichtungen zum Abfangen elektromagnetischer Abstrahlung von Tastaturen.[499]

Im Zusammenhang mit „Hacking-Werkzeugen" ergibt sich die Besonderheit, dass diejenigen Tools, die grundsätzlich legalen Zwecken dienen und iSd § 126c Abs 1 Z 1 dazu geschaffen oder adaptiert wurden (zB Sniffer als Administratoren-Tool), ebenso zur Begehung von Computerstraftaten geeignet sind.[500] Solche Programme werden aufgrund ihrer doppelfunktionalen Verwendungsmöglichkeit als „dual-use-devices" bezeichnet.[501] Nach den Intentionen der Verfasser der CyCC[502] und dem Wortlaut des § 126c sind derartige Tools nicht ersichtlich zur Begehung einer der genannten Computerstraftaten geschaffen oder adaptiert worden, weshalb diese keine verpönten Tatmittel darstellen.[503] Dadurch wird der Anwendungsbereich dieser Strafbestimmung erheblich eingeschränkt.

Bergauer ist der Auffassung, dass eine Unterscheidung zwischen „legalen" und „illegalen" Tools in praxi schwer vorzunehmen ist und kritisiert damit den zu eng gefassten objektiven Tatbestand des § 126c.[504] Seines Erachtens solle der Gesetzgeber eine Umformulierung der betreffenden Passage im Gesetzestext dahingehend vornehmen, dass ein Computerprogramm, gleichgültig zu welchem Zweck es geschaffen oder adaptiert wurde, nach seiner besonderen Beschaffenheit ersichtlich zur Begehung einer der genannten Straftaten „geeignet" sein muss.[505] Darüber hinaus bemerkt *Bergauer*, dass nach dem Vorbild des

---

[497] *Bergauer* in BMJ, 35. Ottensteiner Fortbildungsseminar aus Strafrecht und Kriminologie, 27 (31); *Bergauer*, Phishing im Internet – eine kernstrafrechtliche Betrachtung, RZ 2006, 82 (87); vgl dazu auch *Reindl-Krauskopf* in WK-StGB² § 126c Rz 7.
[498] Vgl dazu *Reindl-Krauskopf* in WK-StGB² § 126c Rz 8; ErlRV 1166 BlgNR XXI. GP, 29 f.
[499] *Reindl-Krauskopf* in WK-StGB² § 126c Rz 9.
[500] *Bergauer*, ÖJZ 2007/45, 532 (533).
[501] *Daxecker* in SbgK § 126c Rz 18.
[502] Explanatory Report Z 73.
[503] *Daxecker* in SbgK § 126c Rz 18 f; *Reindl-Krauskopf* in WK-StGB² § 126c Rz 8.
[504] *Bergauer*, ÖJZ 2007/45, 532 (533 f).
[505] *Bergauer*, ÖJZ 2007/45, 532 (534).

Art 6 Abs 2 CyCC der Tatbestand um das Merkmal „unbefugt“ erweitert werden sollte, weil auch IT-Sicherheitsunternehmen derartige Computerprogramme herstellen oder besitzen, um Systeme von Kunden auf Schwachstellen zu testen.[506]

Nach *Bertel/Schwaighofer* sollten von § 126c nur solche Computerprogramme bzw Zugangsdaten erfasst werden, die „keinem anderen legalen Zweck dienen können“.[507] *Bergauer* kritisiert diese Auffassung mE zu Recht, da „bösartige“ Programme, die zum Zweck der Begehung eines der vorbereitenden Delikte hergestellt wurden, von § 126c Abs 1 Z 1 im Hinblick auf eine legale Verwendungsmöglichkeit als Administratoren-Werkzeug nicht erfasst wären.[508] Dies ist bspw bei Remote-Access-Tools der Fall, die als Fernwartungssoftware auch von Systemadministratoren eingesetzt werden und damit legalen Zwecken dienen können.

5.5.2.3.2. Computerpasswörter, Zugangscodes und vergleichbare Daten

Als Tatobjekte erfasst § 126c Abs 1 Z 2 Authentifizierungsdaten aller Art, die den Zugriff auf Systeme oder Teile davon ermöglichen.[509] Unter diesem weit zu verstehenden Begriff fallen sämtliche Passwörter, ob verschlüsselt oder unverschlüsselt, die den Zugriff auf Benutzerkonten ermöglichen. Daneben sind auch PIN-Codes, die vorwiegend als Zugriffssperren für mobile Internetzugänge bzw Mobiltelefone zum Einsatz kommen, als Zugangsdaten iSd Abs 1 Z 2 zu qualifizieren.

5.5.2.4. Tathandlungen

5.5.2.4.1. Herstellen

Die Tathandlung des Herstellens bezeichnet die Produktion von Tatmitteln und erfasst sowohl die Herstellung körperlicher Vorrichtungen (zB Abhöranlagen), sowie das Programmieren von „bösartigen“ Computerprogrammen (Computerwürmer, Sniffer udgl).[510] Das geschaffene Tatmittel muss im Wesentlichen gebrauchsfertig sein.[511] Nach *Bergauer* liegt die Tathandlung des Herstellens vor, wenn ein bereits fertiggestelltes und einsatzfähiges Schadprogramm vervielfältigt wird.[512]

---

506 *Bergauer*, ÖJZ 2007/45, 532 (534 f).
507 Siehe dazu *Bertel/Schwaighofer*, Österreichisches Strafrecht Besonderer Teil I (§§ 75 bis 168)[12] (2012) 186.
508 *Bergauer*, ÖJZ 2007/45, 532 (534).
509 *Reindl-Krauskopf* in WK-StGB[2] § 126c Rz 10; *Daxecker* in SbgK § 126c Rz 21.
510 *Reindl-Krauskopf* in WK-StGB[2] § 126c Rz 11.
511 *Daxecker* in SbgK § 126c Rz 23.
512 *Bergauer* in Hinterhofer/Schütz, Fallbuch Straf- und Strafprozessrecht, 141 (150).

5.5.2.4.2. Einführen

Der Begriff „Einführen“ erfasst den Import eines verpönten Tatmittels über die Staatsgrenze nach Österreich. Als tatbildliche Handlung kommt sowohl die elektronische Übermittlung (zB das Versenden eines E-Mails von einem ausländischen auf einen inländischen Server) als auch die Verbringung des Tatmittels auf anderem Wege (zB der Versand eines infizierten USB-Sticks mit dem Paketdienst) in Betracht.[513]

5.5.2.4.3. Vertreiben, Veräußern, Sonst-Zugänglichmachen

Den Tathandlungen des Vertreibens, Veräußerns oder Sonst-Zugänglichmachens unterfallen sämtliche Arten der Verbreitung verpönter Tatmittel.[514] Die Tathandlung des Sonst-Zugänglichmachens erfüllt dabei eine Art Auffangfunktion und erfasst jede sonstige Verteilung.[515] Darunter fallen Verhaltensweisen wie etwa das Platzieren spezieller DDoS-Tools auf Webseiten, das Versenden von Schadsoftware via E-Mails sowie die Veröffentlichung zuvor „gehackter“ Zugangscodes (zB Passwortlisten). Ob die Verteilung daher entgeltlich (zB durch Online-Verkäufe) oder unentgeltlich (zB kostenfreie Downloads) erfolgt, ist unerheblich.[516]

5.5.2.4.4. Sich-Verschaffen und Besitzen

Das Sich-Verschaffen und der Besitz wurden mit dem StRÄG 2004 in den objektiven Tatbestand des § 126c aufgenommen.[517] Die Tathandlung des Sich-Verschaffens verlangt zur Gewahrsamserlangung das eigene Zutun des Täters, bspw durch einen Mausklick auf den Download-Knopf.[518] Im Unterschied dazu ist der Besitz auch dann strafbar, wenn ein Tatmittel ohne Zutun des Täters in seinen Gewahrsam gelangt, bspw durch den Empfang eines E-Mails. Insofern stellt der Besitz eine schlichte Tätigkeit dar.[519]

Zur Tathandlung des Sich-Verschaffens von Zugangsdaten führt *Bergauer* näher aus, dass es sich nicht um eine Gewahrsamserlangung im strengen strafrechtlichen Sinn handeln kann.[520] Seines Erachtens handelt der Täter auch dann tatbestandsmäßig, wenn er die Schreibtischlade öffnet und sich das auf einem Zettel notierte Passwort merkt, ohne das Papier wegzunehmen und in seinen Gewahrsam zu bringen.

---

513 *Daxecker* in SbgK § 126c Rz 24.
514 *Reindl-Krauskopf* in WK-StGB² § 126c Rz 11.
515 *Daxecker* in SbgK § 126c Rz 25.
516 *Daxecker* in SbgK § 126c Rz 25.
517 *Daxecker* in SbgK § 126c Rz 6.
518 *Daxecker* in SbgK § 126c Rz 26.
519 *Bergauer* in Hinterhofer/Schütz, Fallbuch Straf- und Strafprozessrecht, 141 (150).
520 *Bergauer*, jusIT 2012/93, 199 (200).

5.5.3. Subjektiver Tatbestand

Der Tatbildvorsatz muss sämtliche objektiven Tatbestandsmerkmale (insb die besondere Beschaffenheit der Tatobjekte zur Begehung der angeführten Delikte) umfassen und zumindest im Stärkegrad des dolus eventualis vorliegen.[521] § 126c verlangt vom Täter zusätzlich zum Tatbestandsvorsatz einen erweiterten Vorsatz, die Tatmittel zur Begehung einer der in Abs 1 Z 1 leg cit genannten Delikte verwenden zu wollen. Auch im Bereich des erweiterten Vorsatzes genügt dolus eventualis.[522] Eine tatsächliche Nutzung des verpönten Tatmittels wird für die Strafbarkeit allerdings nicht verlangt.[523]

Darüber hinaus muss der Vorsatz des Täters auch auf die Verwirklichung eines der in § 126c genannten Delikte gerichtet sein und somit den Tatbestandsvorsatz sowie auch einen deliktsspezifischen erweiterten Vorsatz dieser Strafbestimmung umfassen.[524] In Bezug auf den überschießenden Vorsatz ergeben sich keine besonderen Anforderungen an den Stärkegrad, sodass dolus eventualis ausreicht.[525] Nach *Reindl-Krauskopf* wird eine genaue Kenntnis des Tatplans nicht zu verlangen sein.[526]

5.5.4. Besonderheiten

5.5.4.1. Vollendung und Versuch

Ein strafbarer Versuch gem § 15 ist bei Vorbereitungsdelikten denkbar und somit auch bezüglich § 126c möglich.[527] Nach *Daxecker* könnte ein strafbarer Versuch vorliegen, wenn ein Programmierer mit der Entwicklung eines Tatmittels (zB eines Computerwurms) beginnt.[528] § 126c ist mit der Fertigstellung oder Beschaffung eines der in Abs 1 leg cit angeführten Tatmittel (zB Trojaner) vollendet, sofern der Täter mit dem erweiterten Vorsatz handelt, dass dieses Programm zur Begehung einer der genannten Straftaten verwendet wird.[529]

5.5.4.2. Beteiligung

Die Beteiligung an § 126c ist nach Maßgabe des § 12 möglich.[530] Als Beitragstäter kommt etwa derjenige in Betracht, der einen Rechner zur Verfügung stellt, um eine neuartige Schadsoftware (zB Computerwurm) zu testen. Bestimmungstäterschaft nach §§ 12 2. Fall iVm

---

521 *Reindl-Krauskopf* in WK-StGB² § 126c Rz 13.
522 *Bergauer*, ÖJZ 2007/45, 532 (534); *Daxecker* in SbgK § 126c Rz 28.
523 *Reindl-Krauskopf* in WK-StGB² § 126c Rz 14.
524 *Reindl-Krauskopf* in WK-StGB² § 126c Rz 15; *Bergauer*, ÖJZ 2007/45, 532 (534).
525 *Bergauer* in Hinterhofer/Schütz, Fallbuch Straf- und Strafprozessrecht, 141 (150).
526 *Reindl-Krauskopf* in WK-StGB² § 126c Rz 15.
527 *Kienapfel/Höpfel/Kert*, Strafrecht AT² Z 21 Rz 7; vgl *Daxecker* in SbgK § 126c Rz 36.
528 *Daxecker* in SbgK § 126c Rz 36.
529 *Daxecker* in SbgK § 126c Rz 36.
530 *Daxecker* in SbgK § 126c Rz 37.

126c ist anzunehmen, wenn jemand einen Malware-Entwickler zur Programmierung eines DDoS-Tool beauftragt, welches zukünftig für Angriffe gegen Web-Server eingesetzt werden soll.

5.5.4.3. Strafaufhebung gem § 126c Abs 2

§ 126c Abs 2 normiert eine Möglichkeit der Strafaufhebung. Diese Regelung wurde einerseits dem Grundgedanken des Rücktritts vom Versuch (§ 16) nachgebildet und hat andererseits Elemente der „Tätigen Reue“ zum Vorbild.[531] Der Täter ist nach § 126c Abs 2 straflos, wenn er freiwillig verhindert, dass Zugangsdaten oder Computerprogramme zur Begehung einer der in Abs 1 leg cit genannten Delikte verwendet werden.[532] Der Rücktritt des Täters ist dann freiwillig, wenn er die Verwendung der Tatmittel etwa aus Angst vor Strafverfolgung endgültig verhindert und damit die Verwendungsgefahr beseitigt, obwohl eine seinem Tatplan entsprechende Benützung des Tatmittels noch möglich gewesen wäre.[533]

Wurde die Gefahr der Verwendung ohne Zutun des Täters beseitigt oder hat eine solche nicht bestanden, ist der Täter gem § 126c Abs 2 nicht zu bestrafen, sofern er sich unabhängig davon freiwillig und ernstlich bemüht, diese zu beseitigen.[534] Der Täter bemüht sich, wenn er alle ihm möglichen Anstrengungen unternimmt, den scheinbar noch möglichen Gebrauch des Tatmittels zu verhindern.[535] Hat die Strafverfolgungsbehörde von der Tat erfahren und handelt der Täter in Unkenntnis über das Wissen der Behörde weiterhin freiwillig, kann er in diesem speziellen Fall straflos werden.[536]

5.5.4.4. Abgrenzungen und Konkurrenzen

Haben die vorbereitenden Delikte des § 126 Abs 1 Z 1 zumindest das Versuchsstadium erreicht, tritt § 126c kraft materieller Subsidiarität hinter diese zurück.[537] Nach den Gesetzesmaterialien ist ein Zusammentreffen der ähnlichen Bestimmungen des § 126c und § 10 ZuKG nicht auszuschließen.[538] Im Hinblick auf die mögliche Verwirklichung beider Delikte soll daher § 126c hinter das speziellere Delikt des § 10 ZuKG zurücktreten.

---

[531] ErlRV 1166 BlgNR XXI. GP, 30; vgl dazu *Reindl-Krauskopf* in WK-StGB^2 § 126c Rz 16; *Daxecker* in SbgK § 126c Rz 32.
[532] *Daxecker* in SbgK § 126c Rz 32.
[533] *Kienapfel/Höpfel/Kert*, Strafrecht AT^{14} Z 23 Rz 14; *Reindl-Krauskopf* in WK-StGB^2 § 126c Rz 17.
[534] *Daxecker* in SbgK § 126c Rz 35.
[535] *Reindl-Krauskopf* in WK-StGB^2 § 126c Rz 19.
[536] *Reindl-Krauskopf* in WK-StGB^2 § 126c Rz 17; zust *Daxecker* in SbgK § 126c Rz 33.
[537] *Daxecker* in SbgK § 126c Rz 38.
[538] ErlRV 1166 BlgNR XXI. GP, 29.

Nach *Reindl-Krauskopf* ist ein Zusammentreffen dieser Delikte kaum denkbar.[539] *Daxecker* vertritt hingegen den Standpunkt, dass durch die Aufnahme des § 148a in den Katalog der vorbereitenden Delikte des § 126c Abs 1 Z 1 eine Konkurrenzsituation sehr wohl denkbar und wahrscheinlich ist.[540]

5.5.5. Anwendbarkeit des § 126c auf Web-Defacements und virtuelle Sit-Ins

5.5.5.1. Objektiver Tatbestand

5.5.5.1.1. Tatsubjekt

Hacktivisten, die verpönte Tatmittel iSd § 126c Abs 1 Z 1 (zB DDoS- oder Brute-Force-Tools) mit dem Vorsatz herstellen, einführen, vertreiben, veräußern, sonst zugänglich machen, sich verschaffen oder besitzen, dass diese zum Zweck der Begehung der genannten Computerstraftaten gebraucht werden, kommen als unmittelbare Täter in Betracht.

5.5.5.1.2. Tatobjekt

Tatobjekte des § 126c sind Computerprogramme und vergleichbare Vorrichtungen (Z 1) bzw jede Art von Computerpasswörtern, Zugangscodes oder vergleichbare Daten (Z 2). Im Vorfeld virtueller Sit-Ins werden automatisierte DDoS-Programme (zB LOIC) auf Webseiten veröffentlicht und durch Protestteilnehmer heruntergeladen. Nach dem Wortlaut des § 126c müssen diese Programme ersichtlich zur Begehung einer der angeführten Straftaten geschaffen oder adaptiert worden sein. Hinsichtlich dieser Einschränkung kann gesagt werden, dass etwa die DDoS-Angriffssoftware „Flood-Net“, welche bei Angriffen auf mexikanische Web-Server zum Einsatz kam, ersichtlich zur Begehung der §§ 126a bzw 126b hergestellt wurde.

5.5.5.1.3. Tathandlung

Werden bspw automatisierte DDoS-Tools von einem Hacktivisten programmiert, ist die Tathandlung des Herstellens verwirklicht, wenn das Tatmittel gebrauchsfertig ist und für Angriffe gegen Web-Server eingesetzt werden kann. Das Sonst-Zugänglichmachen erfüllt etwa derjenige, der dieses Programm auf Webseiten zum kostenfreien Download zur Verfügung stellt. Die Tathandlung des Sich-Verschaffens liegt vor, wenn sich bspw ein Protestteilnehmer das entsprechende Tool auf die Festplatte seines Rechners kopiert.

[539] *Reindl-Krauskopf* in WK-StGB[2] § 126c Rz 20.
[540] *Daxecker* in SbgK § 126c Rz 39.

Die Tatbegehungsvariante des Besitzens ist verwirklicht, wenn das Tool auch ohne Zutun des Täters in seinen Gewahrsam gelangt. Dasselbe gilt für Hacking-Werkzeuge, die im Rahmen von Web-Defacements zum Einsatz kommen.

5.5.5.2. Subjektiver Tatbestand

Zur Verwirklichung des Tatbestandsvorsatzes bzw des erweiterten Vorsatzes genügt dolus eventualis. Stellt ein computertechnisch begabter Hacktivist ein automatisiertes DDoS-Tool her, das ersichtlich zur Begehung des § 126b bzw § 126a geschaffen wurde, und veröffentlicht dieses auf einer von ihm vorgesehenen Webseite, ist er nach § 126c strafbar, sofern er mit dem erforderlichen Eventualvorsatz bezüglich der Tatbegehungsformen des Herstellens und Sonst-Zugänglichmachens sowie auf die besondere Beschaffenheit des Tools zur Begehung des § 126b bzw § 126a handelt. Zudem muss der erweiterte Vorsatz des Täters darauf gerichtet sein, dass dieses Programm zur Begehung eines der in § 126c Abs 1 Z 1 angeführten Delikte verwendet wird. Dh, er muss eine schwere Störung eines Systems, über welches die Programmnutzer nicht oder nicht alleine verfügungsberechtigt sind, ernstlich für möglich halten und sich damit abfinden.[541]

5.5.5.3. Besonderheiten

5.5.5.3.1. Vollendung und Versuch

Das Vorbereitungsdelikt des § 126c ist vollendet, wenn ein Protestteilnehmer das DDoS-Tool mit dem Vorsatz herunterlädt, dieses zur Begehung des § 126a bzw §126b zu verwenden. Ein strafbarer Versuch nach §§ 15, 126c kann vorliegen, wenn ein Schadsoftware-Entwickler mit der Programmierung eines Cracking-Tools beginnt, welches nach der Fertigstellung zur Begehung des § 118a verwendet werden soll.

5.5.5.3.2. Beteiligung

Nach §§ 12 3. Fall, 126c ist als Beitragstäter derjenige anzusehen, der bspw ein Computernetzwerk zur Verfügung stellt, um Computerwürmer oder DDoS-Tools zu testen. Als Bestimmungstäter gem §§ 12 2. Fall, 126c kommt in Betracht, wer einen Malware-Entwickler zur Herstellung eines Hacking-Tools (zB Brute-Force-Programm) beauftragt.

5.5.5.3.3. Strafaufhebung gem § 126c Abs 2

Hacktivisten haben nach § 126c Abs 2 die Möglichkeit der Strafaufhebung, wenn sie die Verwendungsgefahr eines hergestellten DDoS-Tools, welches ersichtlich zur Begehung des

[541] Vgl dazu *Reindl-Krauskopf* in WK-StGB[2] § 126c Rz 15.

§ 126a bzw § 126b geschaffen wurde, freiwillig und endgültig verhindern. Der Täter handelt freiwillig, solange seinem Tatplan entsprechend die Verwendung des Tools möglich ist, er aber dennoch die Gefahr der Verwendung endgültig beseitigt, indem er etwa das Programm unwiderruflich löscht und somit die Verwendung verhindert.[542]

5.5.5.3.4. Abgrenzungen und Konkurrenzen

Sofern die in § 126c Abs 1 Z 1 genannten Delikte das Versuchsstadium erreicht haben, tritt § 126c hinter diese zurück. Dies ist etwa der Fall, wenn ein DDoS-Angriff nicht massiv genug war, den Absturz eines Web-Servers herbeizuführen. Im konkreten Zusammenhang tritt § 126c hinter die versuchte Störung der Funktionsfähigkeit eines Computersystems gem §§15, 126b zurück. Dieses Delikt ist wiederum zur versuchten Datenbeschädigung subsidiär.

5.6. Zusammenfassung

Im Rahmen der vorliegenden Arbeit konnte festgestellt werden, dass im Hinblick auf virtuelle Sit-Ins sowohl § 126a als auch § 126b anwendbar ist. Die Anwendbarkeit des § 126b ist deutlich eingeschränkt, da diese Computerstrafbestimmung aufgrund der in § 126b Abs 1 normierten Subsidiaritätsklausel hinter eine (versuchte) Datenbeschädigung zurücktritt. Sofern durch DDoS-Angriffe keine oder nur geringfügige Schäden herbeigeführt wurden, kommt eine Strafbarkeit wegen versuchter Datenbeschädigung in Betracht. Das Delikt des § 118a ist auf DDoS-Attacken nicht anwendbar, da in solchen Fällen keine tatbildliche Zugangsverschaffung vorliegt. § 126c kommt im Vorfeld derartiger Cyber-Angriffe als spezielles Vorbereitungsdelikt zur Anwendung. In Bezug auf Web-Defacements gelangt primär § 126a zur Anwendung, da mithilfe unterschiedlicher Hacking-Techniken die in einer Datenbank oder auf einem Web-Server gespeicherten Webseiten-Inhalte (Daten iSd § 74 Abs 2) verändert werden. In derartigen Fällen wird idR die Tatbegehungsform der Datenveränderung einschlägig sein. Werden durch das Verunstalten der Webseite keine unmittelbaren Schäden verursacht, kommt die Strafbarkeit wegen Versuchs in Betracht. Der objektive Tatbestand des § 118a kann je nach Angriffsmethode erfüllt sein, wenn eine im System angebrachte spezifische Sicherheitsvorkehrung überwunden wird und sich der Täter den Zugriff zu einem System verschafft. Aufgrund der fehlenden Absicht, die im System gespeicherten Daten in Gewinn- oder Schädigungsabsicht zu verwenden, ist der Stellenwert des § 118a auch im Hinblick auf Web-Defacements als niedrig einzuschätzen. Werden im Vorfeld von Defacement-Attacken „illegale“ Hacking- oder Cracking-Tools hergestellt bzw heruntergeladen, kommt § 126c zur Anwendung.

[542] *Reindl-Krauskopf* in WK-StGB[2] § 126c Rz 17; *Sonntag*, Einführung in das Internetrecht[2], 367 f.

6. Schlussbemerkungen

Die rasante Weiterentwicklung auf dem Gebiet der Computer-, Netzwerk- und Internettechnik hat in den letzten Jahren maßgeblich zur Entstehung neuer Kriminalitätsformen bzw Phänomenen im Internet beigetragen. Aufgrund der neuen Entwicklungen und Trends im Bereich der Internetkriminalität (zB Botnetze) sind insb nationale wie auch internationale Gesetzgeber gezwungen, bereits bestehende Computerstrafdelikte in regelmäßigen Abständen entsprechend anzupassen oder neue Bestimmungen aufzunehmen, um diesen Phänomenen entgegenzuwirken und damit den strafrechtlichen Schutz zu gewährleisten.

Darüber hinaus stellen die zunehmende Verwendung von Anonymisierungsdiensten und die geographische Reichweite des Internet für Strafverfolgungsbehörden besondere Herausforderungen bezüglich der Täterausforschung dar. Dahingehend ist insb im Bereich der Computerkriminalität eine verstärkte internationale Zusammenarbeit zwischen den nationalen Behörden erforderlich.[543]

Im Rahmen der vorliegenden Arbeit wurden neben technischen Grundlagen und Begriffen, das Online-Phänomen „Hacktivismus“ sowie die damit in Verbindung stehenden Akteure beleuchtet. Bemerkenswert ist, dass Hacktivisten im Unterschied zu Online-Kriminellen mit der Durchführung von Cyber-Angriffen in erster Linie politische Ziele verfolgen. Als häufig eingesetzte Protestmethoden sind Web-Defacement- und DDoS-Attacken anzuführen, welche idR gegen ein ausgewähltes Angriffsziel gerichtet sind. Hervorzuheben ist insb das international agierende, nicht erkennbar strukturierte Anonymous-Kollektiv. Diese Vereinigung erlangte durch zahlreiche Cyber-Angriffe auf Webseiten bzw Server die Aufmerksamkeit der Web-Öffentlichkeit. Eine zentrale Rolle spielen soziale Netzwerke (bspw Facebook und Twitter), welche die Kommunikation zwischen den Mitgliedern der Bewegung gewährleisten. Insgesamt kann gesagt werden, dass Hacktivismus ohne Internet keine Existenzgrundlage hätte.

Im Hauptkapitel dieser Arbeit „Computerstrafrechtliche Betrachtung“ erfolgte eine allgemeine Darstellung der speziellen Computerdelikte des Kernstrafrechts (§§ 118a, 126a, 126b und 126c). Im Anschluss wurde analysiert, inwieweit diese Delikte auf ausgewählte Erscheinungsformen des Hacktivismus (Defacement- und DDoS-Attacken) zur Anwendung gelangen. Im konkreten Zusammenhang ist anzumerken, dass die Anwendbarkeit der typischen „Hacking-Bestimmung“ des österreichischen Computerstrafrechts (§ 118a) aufgrund

[543] *Reindl-Krauskopf*, Computerstrafrecht[2], 2.

der objektiven und subjektiven Tatbestandserfordernisse deutlich eingeschränkt wird. Die Subsumtion derartiger Sachverhalte unter dieses Delikt scheitert einerseits an der fehlenden Zugangsverschaffung (virtueller Sit-In) und andererseits an den subjektiven Tatbestandskriterien (Defacement-Angriff).

Hinsichtlich virtueller Sit-Ins sind sowohl § 126a als auch § 126b anwendbar, wobei § 126b aufgrund der Subsidiaritätsklausel hinter § 126a zurücktritt, sofern im Zuge einer Attacke gleichzeitig auch Daten iSd § 126a unterdrückt werden. In Bezug auf Web-Defacements kommt in erster Linie § 126a zur Anwendung. Weiters kann davon ausgegangen werden, dass bezüglich politisch motivierter DDoS-Attacken und Web-Defacements idR ein strafbarer Versuch gem §§ 15 iVm 126a bzw 126b vorliegen wird, weil in vielen Fällen kein unmittelbarer Vermögensschaden iSd § 126a eintritt oder keine schwere Störung iSv § 126b herbeigeführt wird. Demgegenüber pönalisiert das spezielle Vorbereitungsdelikt des § 126c zahlreiche Verhaltensweisen im Vorfeld solcher Cyber-Attacken. Abschließend kann gesagt werden, dass diese Computerstrafdelikte jedenfalls zur strafrechtlichen Beurteilung „hacktivistischer" Sachverhalte heranzuziehen sind.

Quellenverzeichnis

Literaturverzeichnis

Badertscher Kurt/Gubelmann Josef/Scheuring Johannes, Wirtschaftsinformatik Grundlagen: Informations- und Kommunikationssysteme gestalten (Compendio Bildungsmedien 2006)

Beer Johannes, Die Convention on Cybercrime und österreichisches Strafrecht (Trauner Verlag 2005)

Bergauer Christian, Gesetzgebungsmonitor Computerstrafrecht: Ratifikation des Übereinkommens über Computerkriminalität, jusIT 2012/95, 205

Bergauer Christian, Kritische Anmerkungen zu § 126c StGB, ÖJZ 2007/45, 532

Bergauer Christian, Phishing im Internet - eine kernstrafrechtliche Betrachtung, RZ 2006, 82

Bergauer Christian, Rezension Lenard Wengenroth Zur Strafbarkeit von virtuellen Sit-Ins. Zugleich ein Beitrag zur (Mit)Täterschaft bei minimalen Tatbeiträge, jusIT 2014/116, 240

Bergauer Christian, Rezension zu Martin Daxecker in SbgK § 126b und § 126c. Auszug aus Triffterer/Rosbaud/Hinterhofer (Hrsg), Salzburger Kommentar zum StGB, jusIT 2012/93, 199

Bergauer Christian, Sniffer-Tools – unwillkommene Spyware, Ein Sniffer-Angriff unter § 118a StGB subsumiert, RdW 2006/391, 412

Bertel Christian/Schwaighofer Klaus, Österreichisches Strafrecht Besonderer Teil I (§§ 75 bis 168b StGB)[12] (Verlag Österreich 2012)

Birklbauer Alois/Hilf Marianne/Tipold Alexander, Strafrecht Besonderer Teil I[2] (Facultas 2012)

Blumhagel Stefan/Joos Thomas, *Netzwerke: geheime Tricks – perfekt vernetzt! (Markt + Technik Verlag 2005)*

BMJ (Hrsg), 35. Ottensteiner Fortbildungsseminar aus Strafrecht und Kriminologie (NWV 2007)

Eckert Claudia, IT-Sicherheit: Konzepte – Verfahren – Protokolle[6] (Oldenbourg Wissenschaftsverlag 2009)

Ernst Hartmut/Schmidt Jochen/Beneken Gerd, Grundkurs Informatik: Grundlagen und Konzepte für die erfolgreiche IT-Praxis[5] (Springer Vieweg 2015)

Fabrizy Ernst Eugen, Strafgesetzbuch StGB samt ausgewählten Nebengesetzen: Kurzkommentar[11] (Manz 2013)

Fuchs Helmut, Zum Entwurf von Strafbestimmungen gegen die Computerkriminalität, RdW 1985, 330

Fuchs Helmut/Reindl-Krauskopf Susanne, Strafrecht Besonderer Teil I – Delikte gegen den Einzelnen[4] (Verlag Österreich 2014)

Gumm Heinz Peter/Sommer Manfred, Einführung in die Informatik[10] (Oldenbourg Wissenschaftsverlag 2012)

Hinterhofer Hubert/Schütz Hannes (Hrsg), Fallbuch Straf- und Strafprozessrecht (Jan Sramek Verlag 2015)

Höpfel Frank/Ratz Eckart (Hrsg), Wiener Kommentar zum Strafgesetzbuch[2] (Manz 2013)

Jahnel Dietmar/Mader Peter/Staudegger Elisabeth (Hrsg), IT-Recht[3] (Verlag Österreich 2012)

Jarzyna Dirk, TCP/IP: Grundlagen, Adressierung, Subnetting (mitp Verlag 2013)

Jendryschik Michael, Einführung in XHTML, CSS und Webdesign: Standardkonforme, moderne und barrierefreie Websites erstellen[2] (Addison-Wesley Verlag 2009)

Jordan Tim/Taylor Paul, Hacktivism and Cyberwars: Rebels with a Cause (Routledge Verlag 2004)

Kammermann Markus, CompTIA Network+[5] (mitp Verlag 2012)

Kappes Martin, Netzwerk- und Datensicherheit: Eine praktische Einführung[2] (Springer Vieweg 2013)

Kienapfel Diethelm, Grundriß des österreichischen Strafrechts – Besonderer Teil II[3] (Manz 1993)

Kienapfel Diethelm/Höpfel Frank/Kert Robert, Grundriss des Strafrechts Allgemeiner Teil[14] (Manz 2012)

Kmetic Konrad, Grundzüge des Computerstrafrechts (Linde Verlag 2014)

Landler Clara/Parycek Peter/Kettemann Matthias (Hrsg), Netzpolitik in Österreich: Internet. Macht. Menschenrechte. Abschlussbericht 2013 (MV-Verlag 2013)

Maleczky Oskar, Das Strafrechtsänderungsgesetz 2002, JAP 2002/2003, 115

McCaughey Martha/Ayers Michael (Hrsg), Cyberactivism: Online Activism in Theory and Practice (Routledge Verlag 2003)

Mitgutsch Ingrid/Wessely Wolfgang (Hrsg), Handbuch Strafrecht: Besonderer Teil I (Verlag Österreich 2013)

Moschitto Denis/Sen Evrim, Hackerland: Das Logbuch einer Szene[4] (Social Media Verlag 2011)

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

Ortmann Jürgen, Einführung in die PC-Grundlagen[8] (Addison-Wesley Verlag 2003)

Pfister Christa, Hacking in der Schweiz: im Spiegel des europäischen, des deutschen und des österreichischen Computerstrafrechts (Neuer Wissenschaftlicher Verlag 2008)

Reindl-Krauskopf Susanne, Computerstrafrecht im Überblick[2] (facultas.wuv 2009)

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

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

Sambleben Jörg/Schumacher Stefan (Hrsg), Informationstechnologie und Sicherheitspolitik: Wird der dritte Weltkrieg im Internet ausgetragen? (Books on Demand 2012)

Scherff Jürgen, Grundkurs Computernetzwerke: Eine kompakte Einführung in Netzwerk- und Internet-Technologien[2] (Vieweg + Teubner Verlag 2010)

Schmölzer Gabriele, Das neue Computerstrafrecht (Strafrechtsänderungsgesetz 1987), EDVuR 1988 H 1, 20

Seiler Robert, Kritische Anmerkung zum StRÄG 1987 betreffend den Besonderen Teil des StGB, JBl 1989, 746

Sonntag Michael, Die EU-Richtlinie über Angriffe auf Informationssysteme, jusIT 2014/2, 8

Sonntag Michael, Einführung in das Internetrecht – Rechtsgrundlagen für Informatiker[2] (Linde Verlag 2014)

Spenneberg Ralf, Linux-Firewalls mit iptables & Co: Sicherheit mit Kernel 2.4 und 2.6 für Linux-Server und –Netzwerke (Addison-Wesley Verlag 2006)

Studer Bruno, Netzwerkmanagement und Netzwerksicherheit: Ein Kompaktkurs für Praxis und Lehre (vdf Hochschulverlag 2010)

Triffterer Otto/Rosbaud Christian/Hinterhofer Hubert (Hrsg), Salzburger Kommentar zum Strafgesetzbuch (LexisNexis 2012)

Wengenroth Lenard, Zur Strafbarkeit von virtuellen Sit-Ins: Zugleich ein Beitrag zur (Mit)Täterschaft bei minimalen Tatbeiträgen (Duncker & Humblot Berlin 2014)

Winterer Andreas, Windows 7 Sicherheit (bhv-Verlag 2011)

Ziegler Manuel, Web Hacking: Sicherheitslücken in Webanwendungen – Lösungswege für Entwickler (Carl Hanser Verlag 2014)

Nationale Rechtsquellen

Strafgesetzbuch (StGB), BGBl 60/1974

Datenschutzgesetz (DSG), BGBl 565/1978

Datenschutzgesetz 2000 (DSG 2000), BGBl I 165/1999

Bundesgesetz über den Schutz zugangskontrollierter Dienste (Zugangskontrollgesetz - ZuKG), BGBl I 60/2000

Strafrechtsänderungsgesetz 2002, BGBl I 134/2002

Telekommunikationsgesetz 2003 (TKG 2003), BGBl I 70/2003

Strafrechtsänderungsgesetz 2004, BGBl I 15/2004

Strafrechtsänderungsgesetz 2008, BGBl I 109/2007

Gesetzesmaterialien

JAB 359 BlgNR XVII. GP

ErlRV 1166 BlgNR XXI. GP

ErlRV 309 BlgNR XXII. GP

ErlRV 285 BlgNR XXIII. GP

ErlRV 689 BlgNR XXV. GP

Internationale Rechtsquellen

Rahmenbeschluss 2001/413/JI des Rates vom 28.5.2001 zur Bekämpfung von Betrug und Fälschung im Zusammenhang mit unbaren Zahlungsmitteln, ABl L 2001/149

Convention on Cybercrime des Europarates vom 23. November 2001, ETS 185

Explanatory Report zur Convention on Cybercrime des Europarates vom 23. November 2001, ETS 185

Rahmenbeschluss 2005/222/JI des Rates vom 24. Februar 2005 über Angriffe auf Informationssysteme, ABl L 2005/69

Richtlinie 2013/40/EU des Europäischen Parlaments und des Rates vom 12. August 2013 über Angriffe auf Informationssysteme und zur Ersetzung des Rahmenbeschlusses 2005/222/JI des Rates, ABl L 2013/218

Internetquellen

<anonhq.com/anonymous-hacktivists-strike-blow-isis/> (1.12.2014)

<big-social-media.de/news_publikationen/meldungen/2012_06_04_Shitstorm.php> (5.10.2014)

<blog.emagined.com/2009/05/08/the-five-phase-approach-of-malicious-hackers/> (4.10.2014)

<blog.kaspersky.de/was-ist-ein-rootkit/853/> (19.10.2014)

<catb.org/jargon/html/C/cracker.html> (30.11.2014)

<catb.org/jargon/html/H/hacker.html> (13.11.2014)

<catb.org/jargon/html/H/hacker-ethic.html> (13.11.2014)

<catb.org/jargon/html/S/script-kiddies.html> (13.11.2014)

<ccc.de/de/hackerethik> (13.11.2014)

<chanology-wiki.info/anonymous#projekt-chanology> (23.11.2014)

<cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160> (14.10.2014)

<de.wikipedia.org/wiki/Anonymous_(Kollektiv)> (22.11.2014)

<de.wikipedia.org/wiki/Defacement> (7.10.2014)

<de.wikipedia.org/wiki/Hacker_(Computersicherheit)> (3.10.2014)

<de.wikipedia.org/wiki/Hacker> (3.10.2014)

<de.wikipedia.org/wiki/Hacktivismus> (22.9.2014)

<de.wikipedia.org/wiki/Online-Demonstration> (6.10.2014)

<derstandard.at/1295571047625/Wegen-Protesten-Aegyptische-Regierung-schaltet-Internet-ab> (9.12.2014)

<derstandard.at/1308680131769/Naechtlicher-Ueberfall-Anonymous-attackiert-Seiten-von-SPOe-und-FPOe> (23.11.2014)

<derstandard.at/2000002393084/Sexismus-Shitstorm-gegen-Heinisch-Hosek> (6.10.2014)

<digitales.oesterreich.gv.at/site/6351/default.aspx> (25.4.2015)

<duden.de/rechtschreibung/Nickname> (4.10.2014)

<duden.de/rechtschreibung/Shitstorm> (5.10.2014)

<en.wikipedia.org/wiki/Doxing> (8.10.2014)

<en.wikipedia.org/wiki/WANK_(computer_worm)> (1.12.2014)

<facebook.com> (4.10.2014)

<futurezone.at/netzpolitik/diese-seiten-machen-beim-internet-blackout-mit/24.574.845> (5.10.2014)

<gohacking.com/what-is-doxing-and-how-it-is-done/> (8.10.2014)

<hack-tools.blackploit.com/2014/02/havij-117-automated-and-advanced-sql.html> (9.12.2014)

<heise.de/ct/artikel/Das-Sicherheitsloch-285320.html> (13.10.2014)

<heise.de/ct/artikel/Operation-Payback-Proteste-per-Mausklick-1150151.html> (9.12.2014)

<heise.de/security/artikel/Giftspritze-270382.html> (13.10.2014)

<heise.de/security/artikel/So-funktioniert-der-Heartbleed-Exploit-2168010.html> (14.10.2014)

<heise.de/security/meldung/Anonymous-neue-Waffe-1418014.html> (9.12.2014)

<heise.de/security/meldung/Stuxnet-Gemeinschaftsprojekt-der-USA-und-Israels-1170175.html> (9.10.2014)

<heise.de/tp/artikel/1/1461/1.html> (6.10.2014)

<ikarussecurity.com/at/support/infos-tipps/sicherheitsempfehlungen/hacking-praevention-und-handling/> (9.10.2014)

<itwissen.info/definition/lexikon/Computer-computer.html> (10.9.2014)

<itwissen.info/definition/lexikon/content-management-system-CMS-Content-Managementsystem.html> (19.9.2014)

<itwissen.info/definition/lexikon/denial-of-service-DoS-DoS-Attacke.html> (27.9.2014)

<itwissen.info/definition/lexikon/Personal-Computer-PC-personal-computer.html> (10.9.2014)

<itwissen.info/definition/lexikon/Phreaking-phreaking.html> (13.11.2014)

<itwissen.info/definition/lexikon/Ransomware-ransomware.html> (1.12.2014)

<itwissen.info/definition/lexikon/Soziales-Netzwerk-social-network.html> (19.9.2014)

<itwissen.info/definition/lexikon/Spyware-spyware.html> (1.12.2014)

<kurier.at/lebensart/technik/amazon-skandal-verursacht-protestwelle-und-boykott-aufrufe-im-netz/3.671.631> (5.10.2014)

<kurier.at/lebensart/technik/anonymous-attackiert-tuerkische-websites/715.651> (10.12.2014)

<nmap.org/download.html> (19.10.2014)

<pastebin.com/sHL5W4Rd> (23.11.2014)

<pastebin.com> (7.10.2014)

<rfc-editor.org/> (16.9.2014)

<rfc-editor.org/rfc/rfc2131.txt> (18.9.2014)

<rfc-editor.org/rfc/rfc3207.txt> (18.9.2014)

<rfc-editor.org/rfc/rfc5336.txt> (18.9.2014)

<rfc-editor.org/rfc/rfc7230.txt> (18.9.2014)

<rfc-editor.org/rfc/rfc791.txt> (16.9.2014)

<rfc-editor.org/rfc/rfc792.txt> (16.9.2014)

<rfc-editor.org/rfc/rfc793.txt> (16.9.2014)

<salzburg.com/nachrichten/salzburg/chronik/sn/artikel/anonymous-hackt-website-des-altstadtverbands-123551/> (23.11.2014)

<sans.edu/research/security-laboratory/article/hybrid-threats-did> (1.12.2014)

<sea.sy/index/en> (9.12.2014)

<sea.sy/Latest_Hacks_EN> (10.12.2014)

<sectools.org/tool/john/> (20.10.2014)

<sectools.org/tool/nessus/> (19.10.2014)

<sicherheitskultur.at/Angreifer_im_Internet.htm> (9.10.2014)

<sicherheitskultur.at/Pen_tests.htm> (4.10.2014)

<spiegel.de/netzwelt/web/operation-payback-hacker-grossangriff-auf-mastercard-visa-co-a-733520.html> (1.12.2014)

<spiegel.de/politik/ausland/hackerangriffe-usa-beschuldigen-china-der-cyber-spionage-a-898446.html> (9.10.2014)

<spiegel.de/spiegel/a-791039.html> (9.12.2014)

<spiegel.de/spiegel/a-791039-2.html> (9.12.2014)

<teltarif.de/hacker-angriff-2011-rueckblick-ausblick-2012/news/44946.html> (23.9.2014)

<torproject.org/about/overview.html.en> (20.11.2014)

<twitter.com/hashtag/opisis> (1.12.2014)

<twitter.com/youranonnews> (22.11.2014)

<twitter.com> (4.10.2014)

<who.is> (19.10.2014)

<youtube.com/watch?v=fL3_4tsG_Ig> (8.10.2014)

<youtube.com> (4.10.2014)

<zone-h.org/archive> (7.10.2014)

Bu Zheng/Bueno Pedro/Kashyap Rahul/Wosotowsky Adam, Das neue Zeitalter der Botnets <mcafee.com/de/resources/white-papers/wp-new-era-of-botnets.pdf> (23.11.2014)

Bundeskanzleramt, Bericht Cyber Sicherheit 2014 <bka.gv.at/DocView.axd?CobId=55935> (8.10.2014)

Bundeskriminalamt, Cybercrime in Österreich: Report 2013 <bmi.gv.at/cms/BK/presse/files/Cybercrime_Report_2013.pdf> (26.10.2014).

Bundeskriminalamt, Hacktivisten: Abschlussbericht zum Projektteil der Hellfeldbeforschung <bka.de/> (1.2.2015)

Denning Dorothy, Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy <faculty.nps.edu/dedennin/publications/Activism-Hacktivism-Cyberterrorism.pdf> (23.9.2014)

Imperva, Hacker Intelligence Summary Report: The Anatomy of an Anonymous Attack <imperva.com/download.asp?id=312> (1.12.2014)

NetSecure-IT, Google Hacking <whitepaper.netsecure-it.de/Whitepaper_Google_Hacking.pdf> (3.12.2014)

NetSecure-IT, Whitepaper „Hackerdefinition“: Hacker (Motive) und Angriffstechniken <whitepaper.netsecure-it.de/Hackerdefinition.pdf> (4.10.2014)

Paget François, Hacktivismus: Das Internet ist das neue Medium für politische Stimmen <mcafee.com/de/resources/white-papers/wp-hacktivism.pdf> (20.9.2014)