GESETZENTWURF ZUM SOG. «DIGITALEN HAUSFRIEDENSBRUCH»: NOTWENDIGE SCHLIEßUNG VON STRAFBARKEITSLÜCKEN ODER SYMBOLGESETZGEBUNG?

Michael Busching

Wissenschaftlicher Mitarbeiter, Universität Konstanz, Fachbereich Rechtswissenschaft
Universitätsstraße 10, 78464 Konstanz, DE
michael.busching@uni-konstanz.de

Schlagworte: ***Digitaler Hausfriedensbruch, Strafrechtlicher Datenschutz, Botnetze, Cybercrime-Konvention, EU-Richtlinie über Angriffe auf Informationssysteme***

Abstract: *In Österreich schützt § 118a StGB unter Umsetzung der Cybercrime-Konvention den widerrechtlichen Zugriff auf ein System. Der deutsche § 202a StGB pönalisiert hingegen nicht den Zugriff auf ein System, sondern das Verschaffen eines Zugangs zu Daten. Daher wird aktuell die Einführung eines Straftatbestands (§ 202e StGB-E) zum sog. digitalen Hausfriedensbruch diskutiert. Der Beitrag untersucht, ob diese Einführung aufgrund von bestehenden Strafbarkeitslücken, einem mangelnden Rechtsgüterschutz oder europarechtlichen Vorgaben tatsächlich notwendig ist.*

1. Einleitung

Am 23. November 2001 wurde in Budapest das Übereinkommen des Europarats über Computerkriminalität[1] (sog. «Convention on Cybercrime» bzw. Cybercrime-Konvention) unterzeichnet. Dessen Art. 2 verpflichtet die Vertragsparteien und damit auch die Bundesrepublik Deutschland, «den unbefugten Zugang zu einem Computersystem als Ganzem oder zu einem Teil davon, wenn vorsätzlich begangen, […] als Straftat zu umschreiben».[2] Eine fast wortgleiche Verpflichtung findet sich zudem in der EU-Richtlinie über Angriffe auf Informationssysteme.[3] In Österreich existiert mit § 118a StGB ein Straftatbestand, der den widerrechtlichen Zugriff auf ein Computersystem unter Strafe stellt und damit die europäischen Vorgaben umsetzt. In Deutschland erscheint die Rechtslage in diesem Bereich prima vista hingegen nicht so eindeutig, da der deutsche § 202a StGB nicht primär den Zugriff auf ein Computersystem, sondern das unbefugte Verschaffen eines Zugangs zu Daten unter Strafe stellt.

Der deutsche Bundesrat hat nunmehr am 23. September 2016, auf Initiative des Landes Hessen, einen Gesetzentwurf[4] zu einem Strafrechtsänderungsgesetz beschlossen, welcher die Schaffung eines neuen § 202e StGB zur Strafbarkeit der unbefugten Benutzung informationstechnischer Systeme – sog. «digitaler Hausfriedensbruch» – zum Inhalt hat.[5] Der Vorschlag verfolgt u.a. das Ziel, die Cybercrime-Konvention vollständig umzusetzen,[6] was durch die bisherigen Vorschriften aus dem Kernstrafrecht nach Auffassung des Landes Hessen

---

1 Abgedruckt in BGBl. 2008 II Nr. 30, 1242.

2 Vgl. BGBl. 2008 II Nr. 30, 1242 (1246 f.); siehe hierzu auch bereits Mavany, Pferde, Würmer, Roboter, Zombies und das Strafrecht? Vom Sinn und Unsinn neuer Gesetze gegen den sog. digitalen Hausfriedensbruch, KriPoZ 2016, S. 106 (S. 106 f.).

3 Richtlinie 2013/40/EU, ABl. EU L 218, 8.

4 BT Drs. 18/10182.

5 Vgl. etwa auch schon die Ausführungen bei Mavany, Digitaler Hausfriedensbruch – Allheilmittel oder bittere Pille?, ZRP 2016, S. 221 (S. 222).

6 BT Drs. 18/10182, 11.

nicht geschehen sei.[7] Daneben wird durch das Gesetz angestrebt, einen Schutz des vom BVerfG[8] postulierten Grundrechts «auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme» zu schaffen[9] sowie bestehende Strafbarkeitslücken zu schließen.[10] Angesichts der bereits existierenden Vorschriften im Strafgesetzbuch – insb. § 202a StGB – stellt sich daher die Frage, ob die Einführung eines zusätzlichen Tatbestands zum «digitalen Hausfriedensbruch» tatsächlich erforderlich ist.[11]

2. Technische und begriffliche Hintergründe

Zu einem großen Teil stützt der Bundesrat seine Argumentation zur Notwendigkeit des § 202e StGB-E auf die bisherige Straflosigkeit des Aufbaus, Betriebs und der Nutzung von sog. «Botnetzen».[12] Um diese Argumentation nachvollziehen und überprüfen zu können, muss daher zunächst geklärt werden, was unter einem solchen «Botnetz» überhaupt zu verstehen ist.[13] Der Begriff setzt sich zusammen aus «Bot» (vom englischen «Robot»)[14] und «Netz» und umschreibt damit den Zusammenschluss von mit dem Internet verbundenen informationstechnischen Systemen, die aufgrund einer Infizierung mit Schadsoftware unbemerkt ferngesteuert werden können.[15] Diese einzelnen Teile des Botnetzes werden als «Bots» bezeichnet und können bspw. PCs, Smartphones, Router oder SMART TVs sein.[16] Oftmals werden solche Systemverbünde zum Versand von Spam[17] oder für DDos-Attacken[18] eingesetzt.[19] Neben der persönlichen Nutzung derselben erfolgt inzwischen auch oftmals eine Weitervermarktung an Dritte als eine Art «Botnet as a Service».[20] So dienen Botnetze mehr und mehr als elementare Infrastruktur im Bereich der Computerkriminalität.[21]

Betrachtet man den Ablauf vom Aufbau eines Botnetzes bis hin zu dessen Verwendung, so lassen sich im Wesentlichen drei Phasen unterscheiden:[22] Das Programmieren der Schadsoftware (1. Phase), die Infizierung der einzelnen Systeme (2. Phase) sowie die Verwendung des Netzes für weitere Straftaten (3. Phase).

3. Strafbarkeitslücken nach bisher geltendem Recht

Nachdem nun die technischen Hintergründe geklärt wurden, soll in einem nächsten Schritt überprüft werden, ob die behaupteten Strafbarkeitslücken im Zusammenhang mit Botnetzen sowie anderen im Gesetzentwurf genannten Konstellationen tatsächlich existieren, um so der Antwort auf die Frage nach der tatsächlichen Notwendigkeit einer Erweiterung des Strafrechts näher zu kommen.

---

7 BT Drs. 18/10182, 11 f.

8 BVerfG, Urteil vom 27. Februar 2008, 1 BvR 370/07, 1 BvR 595/07. In: MMR 2008, S. 315.

9 BT Drs. 18/10182, 11.

10 BT Drs. 18/10182, 3 ff.

11 Hierzu kritisch u.a. bereits Mavany, KriPoZ 2016, S. 106; Buermeyer, «Digitaler Hausfriedensbruch»: IT-Strafrecht auf Abwegen, http://www.lto.de/recht/hintergruende/h/entwurf-straftatbestand-digitaler-hausfriedensbruch-botnetze-internet/ (alle Internetquellen abgerufen am 9. Januar 2017); Mavany, ZRP 2016, S. 221; Biselli, Digitaler Hausfriedensbruch: Hessen will neuen Straftatbestand gegen bereits illegale Botnetze einführen, https://netzpolitik.org/2016/digitaler-hausfriedensbruch-hessen-will-neuen-straftatbestand-gegen-bereits-illegale-botnetze-einfuehren/; BT Drs. 18/10182, 19.

12 BT Drs. 18/10182, 1 ff.

13 Vgl. hierzu auch schon ausführlich Mavany, KriPoZ 2016, S. 106 (S. 107 f.).

14 G DATA Software AG, Was ist eigentlich ein Botnet?, https://www.gdata.de/ratgeber/was-ist-eigentlich-ein-botnet; BT Drs. 18/10182, 2.

15 BT Drs. 18/10182, 1 f.; Mavany, ZRP 2016, S. 221 (S. 221); Mavany, KriPoZ 2016, S. 106 (S. 107).

16 Mavany, KriPoZ 2016, S. 106 (S. 107).

17 Siehe zum Begriff etwa Wikipedia, Spam, https://de.wikipedia.org/wiki/Spam.

18 Siehe zum Begriff Wikipedia, Denial of Service, https://de.wikipedia.org/wiki/Denial_of_Service.

19 G DATA Software AG, a.a.O.; BT Drs. 18/10182, 2; Mavany, KriPoZ 2016, S. 106 (S. 107); Biselli, a.a.O.

20 Buermeyer, a.a.O.; Buermeyer/Golla, «Digitaler Hausfriedensbruch» – Der Entwurf eines Gesetzes zur Strafbarkeit der unbefugten Benutzung informationstechnischer Systeme, K&R 2017, S. 14 (S. 14).

21 BT Drs. 18/10182, 2; Mavany, KriPoZ 2016, S. 106 (S. 107).

22 So auch schon überzeugend Mavany, KriPoZ 2016, S. 106 (S. 108); in vier Schritte einteilend auch schon Buermeyer/Golla, a.a.O., S. 15.

3.1. Strafbarkeit de lege lata im Zusammenhang mit Botnetzen[23]

Hierbei bietet sich in Bezug auf Botnetzkriminalität die bereits oben[24] angesprochene Einteilung der unterschiedlichen Handlungen in drei Phasen an.[25] Vor diesem Hintergrund befasst sich der «digitale Hausfriedensbruch» mit der zweiten Phase, in der einzelne Systeme mit einer Schadsoftware infiziert und so zu «Bots» werden,[26] wobei nach bisherigem Recht v.a. eine Strafbarkeit nach § 202a StGB in Betracht kommt.[27]

§ 202a StGB stellt das unbefugte Verschaffen eines Zugangs zu Daten unter Strafe, die nicht für den Täter bestimmt und gegen unberechtigten Zugang besonders gesichert sind.[28] Unter Daten werden in diesem Zusammenhang allgemein alle durch Zeichen oder kontinuierliche Funktionen dargestellten Informationen erfasst, die sich als Gegenstand oder Mittel der Datenverarbeitung für eine Datenverarbeitungsanlage codieren lassen.[29] Diese müssen ferner elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sein oder übermittelt werden (§ 202a Abs. 2 StGB), wobei es auf deren Inhalt gerade nicht ankommt.[30] Mithin erfasst § 202a StGB jegliche auf einem informationstechnischen System befindlichen Informationen, auch bspw. solche des Betriebssystems. Das Erlangen eines Zugangs zu bestimmten (gar sensiblen) Daten ist folglich nicht notwendig.

Eine Strafbarkeit nach § 202a StGB erfordert in Bezug auf die hier untersuchte Konstellation jedoch, dass die betroffenen Daten nicht für denjenigen bestimmt sind, der ein System mittels Schadsoftware zum Bot macht. Dies ist der Fall, wenn sie nach dem Willen des Verfügungsberechtigten nicht in den Herrschaftsbereich des Täters gelangen sollen,[31] wovon regelmäßig auszugehen ist, da die Infizierung mit Schadsoftware typischerweise gegen den Willen des Berechtigten erfolgt. Aus diesem Grund wird die Schadsoftware in aller Regel auch gerade unbemerkt vom jeweiligen Nutzer des Systems installiert.

Außerdem müsste der Botnetzbetreiber als Täter eine Zugangssicherung überwinden.[32] Hierzu zählen alle Vorkehrungen, die subjektiv (zumindest auch) gerade dem speziellen Zweck dienen, den Zugriff durch Unberechtigte zu verhindern oder zumindest nicht unerheblich zu erschweren und zudem objektiv hierzu geeignet sind.[33] Bei gespeicherten Daten sind dies nicht nur unmittelbar an den Daten ansetzende Vorkehrungen, wie etwa eine Verschlüsselung, sondern auch mittelbare Sicherungen, bspw. Systempasswörter oder der Betrieb einer Firewall bzw. Antivirensoftware.[34] Abgesehen davon, dass derartige Sicherungen in der Praxis nahezu immer vorhanden sind und die Infizierung, schon um unbemerkt zu bleiben, typischerweise unter Ausnutzung von Sicherheitslücken erfolgt,[35] soll auch nach § 202e StGB-E das Überwinden einer Sperre notwendig sein, sodass die Unterschiede von § 202a StGB und § 202e StGB-E in diesem Bereich allenfalls theoretischer Na-

---

23 Vgl. hierzu auch schon die Ausführungen bei Mavany, KriPoZ 2016, S. 106.

24 Vgl. Kapitel 2.

25 Siehe zur Einteilung in drei Phasen auch schon Mavany, KriPoZ 2016, S. 106 (S. 108); vier Schritte unterscheidend bereits Buermeyer/Golla, a.a.O., S. 15; eine Differenzierung der einzelnen Handlungen vornehmend zudem u.a. schon Roos/Schumacher, Botnetze als Herausforderung für Recht und Gesellschaft, MMR 2014, S. 377.

26 So bereits Mavany, KriPoZ 2016, S. 106 (S. 108).

27 Vgl. hierzu auch schon die ausführliche Untersuchung bei Mavany, KriPoZ 2016, S. 106 (S. 108 ff.); siehe ferner bereits Roos/Schumacher, a.a.O., S. 379.

28 Malek/Popp, Strafsachen im Internet[2], C.F. Müller, Heidelberg 2015, Rn. 148; Eisele, Computer- und Medienstrafrecht, C.H. Beck, München 2013, § 6 Rn. 3; Mavany, KriPoZ 2016, S. 106 (S. 108); Roos/Schumacher, a.a.O., S. 379.

29 Str. Vgl. hierzu etwa Lenckner/Eisele, § 202a. In: Schönke/Schröder, StGB[29], C.H. Beck, München 2014, § 202a Rn. 3.

30 Vgl. statt vieler Fischer, Strafgesetzbuch mit Nebengesetzen[64], C.H. Beck, München 2017, § 202a Rn. 4.

31 Rengier, Strafrecht Besonderer Teil 2[17], C.H. Beck, München 2016, § 31 Rn. 26.

32 Malek/Popp, a.a.O., Rn. 148; Eisele, a.a.O., § 6 Rn. 3; Mavany, KriPoZ 2016, S. 106 (S. 108).

33 Rengier, a.a.O., § 31 Rn. 27; Fischer, a.a.O., § 202a Rn. 8; Eisele, a.a.O., § 6 Rn. 15; Lenckner/Eisele, a.a.O., § 202a Rn. 14; Mavany, KriPoZ 2016, S. 106 (S. 108).

34 Lenckner/Eisele, a.a.O., § 202a Rn. 15; Mavany, KriPoZ 2016, S. 106 (S. 108); Eisele, a.a.O., § 6 Rn. 15.

35 Buermeyer, a.a.O.

tur sind[36] und die bemängelte Strafbarkeitslücke bei im Einzelfall fehlenden Sicherheitsvorkehrungen auch weiterhin bestehen würde.

Zu guter Letzt setzt eine Strafbarkeit nach § 202a StGB das Erlangen eines unberechtigten[37] Zugangs zu den geschützten Daten voraus. Dafür genügt es, wenn der Täter Daten sichtbar machen kann, also «auf die Daten zugreifen könnte, wenn er wollte».[38] Eine tatsächliche Kenntnisnahme ist hingegen nicht nötig.[39] Nach der gesetzlichen Neufassung des § 202a StGB im Jahr 2007 besteht nun weitestgehend Einigkeit darüber, dass grds. schon das bloße Eindringen in ein Computersystem von der Vorschrift erfasst ist,[40] da in diesen Fällen regelmäßig auch auf Daten zugegriffen werden kann. Straflos wären nach alledem allenfalls Konstellationen, in denen die verwendete Schadsoftware aufgrund ihrer Programmierung nicht in der Lage ist, auf Daten des Systems zuzugreifen.[41] Eine solche Schadsoftware wird jedoch in der Praxis wohl kaum zum Einsatz kommen, da sie zur Begehung weiterer Straftaten mithilfe des Botnetzes nicht sonderlich hilfreich wäre.[42] Daher wird selbst im Gesetzentwurf zur Einführung des § 202e StGB-E darauf hingewiesen, dass «die Kontrolle über die Bots durch den Täter […] vollständig» sei, «d.h. sämtliche auf der Festplatte gespeicherten oder im Arbeitsspeicher befindlichen Daten» dem Täter offen stehen.[43]

Mithin ist das Aufspielen von Trojanern oder ähnlicher Schadsoftware auf ein fremdes Computersystem zum Zwecke der Eingliederung in ein Botnetz regelmäßig nach § 202a StGB strafbar.[44] Teilweise wird in diesem Zusammenhang sogar ausdrücklich von einem «elektronischen Hausfriedensbruch» gesprochen.[45]

Neben § 202a StGB kommen im Zusammenhang mit Botnetzen auch noch weitere Straftatbestände in Betracht.[46] Soweit die Infizierung des fremden Systems z.B. durch Zugriff auf eine Datenübertragung erfolgt, wie etwa über einen infizierten Mailserver, kann außer § 202a StGB auch § 202b StGB erfüllt sein,[47] der das Abfangen von Daten unter Strafe stellt. Ferner wird die Schadsoftware innerhalb der Installationsroutine typischerweise auf Systemdateien zugreifen und diese verändern, womit wiederum eine strafbare Handlung in Form einer Datenveränderung gem. § 303a StGB vorliegt.[48]

Im Übrigen kann sich bei entsprechendem Verwendungsvorsatz auch schon durch das Programmieren der Schadsoftware (1. Phase) eine Strafbarkeit (§ 202c Abs. 1 Nr. 2 StGB) ergeben[49] und auch die Verwendung des Botnetzes (3. Phase) bleibt zumeist nicht straflos.[50] Soweit der Täter bspw. in Bereicherungs- oder Schädigungsabsicht auf einem Bot befindliche personenbezogene Daten verarbeitet (also bspw. übermittelt), macht

---

36 Mavany, ZRP 2016, S. 221 (S. 223 m.w.N.).

37 Die Auslegung des «unberechtigten» Zugangs ist umstritten. Nach richtiger Auffassung dürfte sich hieraus für die Fälle der Botnetzkriminalität keine relevante Einschränkung ergeben. Siehe allgemein zur Diskussion etwa Lenckner/Eisele, a.a.O., § 202a Rn. 17.

38 Mavany, KriPoZ 2016, S. 106 (S. 108).

39 Mavany, KriPoZ 2016, S. 106 (S. 108); Lenckner/Eisele, a.a.O., § 202a Rn. 18; Eisele, a.a.O., § 6 Rn. 19.

40 Vgl. etwa Eisele, a.a.O., § 6 Rn. 18; Lenckner/Eisele, a.a.O., § 202a Rn. 18; Fischer, a.a.O., § 202a Rn. 10a; Rengier, a.a.O., § 31 Rn. 33.

41 Lenckner/Eisele, a.a.O., § 202a Rn. 18; Mavany, KriPoZ 2016, S. 106 (S. 109).

42 Mavany, KriPoZ 2016, S. 106 (S. 109); Mavany, ZRP 2016, S. 221 (S. 223).

43 BT Drs. 18/10182, 2.

44 Vgl. etwa Eisele, a.a.O., § 6 Rn. 19; Lenckner/Eisele, a.a.O., § 202a Rn. 19; Fischer, a.a.O., § 202a Rn. 11; Mavany, KriPoZ 2016, S. 106 (S. 109); Roos/Schumacher, a.a.O., S. 379; Buermeyer/Golla, a.a.O., S. 15.

45 Vgl. etwa Eisele, a.a.O., § 6 Rn. 19 m.w.N.; Buermeyer/Golla, a.a.O., S. 15; Mavany, KriPoZ 2016, S. 106 (S. 109 m.w.N.).

46 Mavany, KriPoZ 2016, S. 106 (S. 109 f.); Mavany, ZRP 2016, S. 221 (S. 222 f.); Buermeyer, a.a.O.; Roos/Schumacher, a.a.O., S. 379 f.

47 Siehe schon Mavany, KriPoZ 2016, S. 106 (S. 109); Roos/Schumacher, a.a.O., S. 379.

48 Mavany, KriPoZ 2016, S. 106 (S. 109); vgl. auch schon Roos/Schumacher, a.a.O., S. 379; Buermeyer/Golla, a.a.O., S. 15; sog. «fileless malware», die keine Daten des Bots verändert, unterfällt, wie vom Gesetzentwurf (BT Drs. 18/10182, 4) angeführt, zwar nicht der Strafbarkeit nach § 303a StGB, dürfte jedoch in tatsächlicher Hinsicht keineswegs die Regel darstellen.

49 Vgl. Buermeyer, a.a.O.; Buermeyer/Golla, a.a.O., S. 15; Mavany, ZRP 2016, S. 221 (S. 222 f.); Roos/Schumacher, a.a.O., S. 379.

50 Siehe zur Einteilung in drei Phasen bereits oben Kapitel 2 sowie Mavany, KriPoZ 2016, S. 106 (S. 108).

er sich nach § 44 Abs. 1 i.V.m. § 43 Abs. 2 Nr. 1, 4 BDSG strafbar.[51] Verwendet er das Botnetz hingegen für sog. DDos-Attacken, liegt regelmäßig ein Fall der nach § 303b StGB strafbaren Computersabotage vor, wie der Gesetzentwurf sogar selbst zugibt.[52] Die ebenfalls vom Gesetzentwurf angesprochenen[53] Krypto-Trojaner, welche Daten verschlüsseln, um «Lösegeld» fordern zu können, führen außerdem zu einer Strafbarkeit nach § 303a bzw. § 253 StGB.[54]

Alles in allem ist damit die Mehrheit der mit Botnetzen verbundenen Handlungen, entgegen der Behauptung des Gesetzentwurfs, bereits nach jetziger Rechtslage strafbar.

3.2. Strafbarkeit de lege lata im Zusammenhang mit weiteren Beispielen

Als weiteres Beispiel für Strafbarkeitslücken wird ferner das Mitlesen einer PIN zur späteren Zugangsverschaffung zu einem Mobiltelefon angeführt.[55] Hier geht es um Fälle, in denen eine Person das spätere Opfer bei der Eingabe der Handy-PIN beobachtet und mit dieser PIN anschließend Zugang zu Daten auf dem Mobiltelefon erlangt. Eine Strafbarkeit nach § 202a StGB scheidet hier nach der im aktuellen Gesetzentwurf vertretenen Ansicht aus, da ein «Überwinden» i.S.v. § 202a StGB einen erheblichen technischen oder zeitlichen Aufwand erfordere.[56] Diese Auffassung ist jedoch alles andere als unumstritten, wie sich aus einer Fußnote des Entwurfs selbst ergibt.[57] So wird ein solcher technischer oder zeitlicher Aufwand vielfach gerade nicht gefordert.[58] Zudem ändert die Beobachtung der PIN-Eingabe auch nichts an der Einordnung derselben als Zugangssicherung.[59] Vielmehr wird man aufgrund der unwillentlichen Preisgabe eine Strafbarkeit nach § 202a StGB sogar bejahen müssen.[60] Hinsichtlich des bloßen Beobachtens der PIN-Eingabe mit dem Vorsatz der späteren Verwendung, dürfte nach dieser Auffassung außerdem § 202c StGB erfüllt sein.[61] Vergleichbares gilt abschließend auch für das Beispiel, in dem ein Botnetzbetreiber das Botnetz einem unabhängig agierenden Dritten für weitere Straftaten zur Verfügung stellt.[62] So bleibt der Dritte aufgrund des neu eingeführten § 202d StGB zur Datenhehlerei, anders als im aktuellen Gesetzentwurf behauptet,[63] nicht zwingend straffrei.[64]

4. Notwendigkeit aufgrund eines unzureichenden Rechtsgüterschutzes

Ferner kann sich die Notwendigkeit der Einführung des § 202e StGB-E jedoch aufgrund eines bislang unzureichenden Rechtsgüterschutzes ergeben.[65] Daran anknüpfend argumentiert der aktuelle Gesetzentwurf, dass das Interesse des Verfügungsberechtigten an der unversehrten Verwendbarkeit von Daten (§§ 202a, 303a StGB) bzw. das Interesse der Betreiber und Nutzer am störungsfreien Funktionieren ihrer Datenverarbeitung (§ 303b StGB) als bisher geschützte Rechtsgüter nicht genügen, um das vom BVerfG[66] postulierte «Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme» ausreichend zu schützen,

---

51 Aus Platzgründen sei hinsichtlich weiterer Einzelheiten auf die Ausführungen von Mavany sowie Roos/Schumacher verwiesen: Mavany, KriPoZ 2016, S. 106 (S. 109); Roos/Schumacher, a.a.O., S. 379.

52 BT Drs. 18/10182, 5; vgl. ferner Roos/Schumacher, a.a.O., S. 379 f.; Mavany, KriPoZ 2016, S. 106 (S. 110); Buermeyer, a.a.O.; Buermeyer/Golla, a.a.O., S. 15.

53 BT Drs. 18/10182, 1.

54 Buermeyer, a.a.O.

55 Vgl. BT Drs. 18/10182, 4.

56 BT Drs. 18/10182, 4.

57 BT Drs. 18/10182, 4 Fn. 5.

58 Vgl. etwa Fischer, a.a.O., § 202a Rn. 11b.

59 Graf, § 202a. In: Joecks/Miebach, Münchener Kommentar zum StGB^2, C.H. Beck, München 2012, § 202a Rn. 42.

60 So bereits überzeugend Mavany, ZRP 2016, S. 221 (S. 222 f. m.w.N.).

61 Buermeyer/Golla, a.a.O., S. 16.

62 BT Drs. 18/10182, 4.

63 BT Drs. 18/10182, 4.

64 Mavany, ZRP 2016, S. 221 (S. 222 f); Buermeyer/Golla, a.a.O., S. 16.

65 BT Drs. 18/10182, 11; Mavany, KriPoZ 2016, S. 106 (S. 110 ff.).

66 BVerfG, Urteil vom 27. Februar 2008, 1 BvR 370/07, 1 BvR 595/07. In: MMR 2008, S. 315.

weshalb ein zusätzlicher Schutz des Interesses der rechtmäßigen Nutzer am ausschließlichen Gebrauchsrecht ihrer Geräte erforderlich sei.[67]

Um diese Argumentation auf ihre Stichhaltigkeit überprüfen zu können, ist es zunächst notwendig, den genauen Inhalt des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme zu betrachten.[68] Hierzu stellte das BVerfG fest, dass der Einzelne zu seiner Persönlichkeitsentfaltung informationstechnischer Systeme bedarf, wobei dem System bei dieser Entfaltung zwangsläufig persönliche Daten anvertraut werden.[69] Dementsprechend sei das Grundrecht nicht per se auf jegliche Systeme anzuwenden, sondern lediglich auf solche, die personenbezogene Daten «in einem Umfang und in einer Vielfalt enthalten können, dass ein Zugriff auf das System es ermöglicht, einen Einblick in wesentliche Teile der Lebensgestaltung einer Person zu gewinnen».[70] Geschützt sei daher «das Interesse des Nutzers, dass die von einem […] System erzeugten, verarbeiteten und gespeicherten Daten vertraulich bleiben.»[71]

Diese Ausführungen zeigen, dass es bei dem genannten Grundrecht letztlich hauptsächlich um die persönlichen Daten des Einzelnen geht, welche er auf einem System verarbeitet. Der Zugriff auf ein System ist vor diesem Hintergrund daher nur zu verbieten, weil dadurch die «entscheidende technische Hürde» für den Zugriff auf persönliche Daten überschritten wird.[72] Im Ergebnis dient es also nichts anderem als dem Interesse des Einzelnen an der Geheimhaltung seiner persönlichen Daten.[73] Aus diesem Grund schließt der an «Daten» und nicht «Systemen» orientierte Wortlaut des § 202a StGB nicht aus, dass die Vorschrift dem Schutz der Vertraulichkeit und Integrität informationstechnischer Systeme dient. Vielmehr schützt dieser das «formalisierte Interesse an der Geheimhaltung von Daten»[74] und damit gerade das, was hinter dem vom BVerfG postulierten Grundrecht steht. Soweit folglich Rechtsgut des § 202e StGB-E das Interesse der rechtmäßigen Nutzer am ausschließlichen Gebrauchsrecht ihrer Geräte sein soll und dieses, in Anlehnung an die Argumentation des Gesetzentwurfs, als Schutz der Vertraulichkeit und Integrität von IT-Systemen verstanden wird, ergibt sich für § 202e StGB-E und § 202a StGB mithin dieselbe Schutzrichtung.[75]

5. Umsetzung der Cybercrime-Konvention sowie der EU-Richtlinie 2013/40/EU

Letztlich führt der aktuelle Gesetzentwurf die Notwendigkeit des § 202e StGB-E noch auf eine bislang unzureichende Umsetzung der Cybercrime-Konvention[76] bzw. der EU-Richtlinie über Angriffe auf Informationssysteme[77] zurück.[78] § 202a StGB wurde jedoch zuletzt im Jahr 2007 geändert, um eben diese Cybercrime-Konvention sowie den EU-Rahmenbeschluss über Angriffe auf Informationssysteme[79] umzusetzen.[80] Letz-

67 BT Drs. 18/10182, 11.

68 Vgl. in diese Richtung letztlich auch schon Mavany, KriPoZ 2016, S. 106 (S. 111 f.).

69 BVerfG, Urteil vom 27. Februar 2008, 1 BvR 370/07, 1 BvR 595/07. In: MMR 2008, S. 315 (318); Mavany, KriPoZ 2016, S. 106 (S. 111).

70 BVerfG, Urteil vom 27. Februar 2008, 1 BvR 370/07, 1 BvR 595/07. In: MMR 2008, S. 315 (318).

71 BVerfG, Urteil vom 27. Februar 2008, 1 BvR 370/07, 1 BvR 595/07. In: MMR 2008, S. 315 (318); vgl. auch Mavany, KriPoZ 2016, S. 106 (S. 111).

72 BVerfG, Urteil vom 27. Februar 2008, 1 BvR 370/07, 1 BvR 595/07. In: MMR 2008, S. 315 (318); Mavany, KriPoZ 2016, S. 106 (S. 111).

73 Mavany, KriPoZ 2016, S. 106 (S. 112).

74 Heger, § 202a. In: Kühl, Strafgesetzbuch Kommentar[28], C.H. Beck, München 2014, § 202a Rn. 2.

75 Daneben wären insb. ein digitales Hausrecht oder gar das Eigentum am jeweiligen System als Schutzgüter des § 202e StGB-E denkbar. Beide sind im Ergebnis allerdings abzulehnen. Vgl. hierzu überzeugend Mavany, KriPoZ 2016, S. 106 (S. 110 f.).

76 BGBl. 2008 II Nr. 30, 1242.

77 Richtlinie 2013/40/EU, ABl. EU L 218, 8.

78 BT Drs. 18/10182, 11 ff.

79 Rahmenbeschluss 2005/222/JI des Rates vom 24. Februar 2005 über Angriffe auf Informationssysteme, ABl. EU L 69, 67.

80 Fischer, a.a.O., § 202a Rn. 1; Lenckner/Eisele, a.a.O., § 202a Rn. 1; Eisele, a.a.O., § 6 Rn. 1; Mavany, KriPoZ 2016, S. 106 (S. 106 f.).

terer wurde schließlich 2013 von der bereits genannten Richtlinie[81] ersetzt, wobei sich die hier relevanten Artikel nahezu wortgleich entsprechen.[82]

Diese europarechtlichen Vorgaben verlangen u.a., dass der unbefugte Zugang zu einem Computersystem, wenn vorsätzlich und unter Verletzung von Sicherheitsmaßnahmen begangen, unter Strafe gestellt wird, sofern kein leichter Fall vorliegt.[83] Dahinter stehen mehrere Überlegungen. Zum einen soll der Tatsache Rechnung getragen werden, dass mögliche Terroranschläge heutzutage auch in der «digitalen Welt» erfolgen können, d.h. Angriffe auf Informationssysteme oder gar kritische Infrastrukturen über das Internet denkbar sind.[84] Zum anderen sollen die Verwendung von Botnetzen, die Störung des Betriebs von Informationssystemen und der Kommunikation sowie das Abgreifen oder Verändern von Daten bekämpft werden.[85]

Fraglich ist, ob diese Vorgaben bereits adäquat durch deutsches Recht umgesetzt wurden,[86] oder ob die Einführung des § 202e StGB-E hierzu tatsächlich notwendig ist. Betrachtet man in diesem Zusammenhang einerseits die genannten Intentionen, lässt sich schon im geltenden deutschen Strafrecht eine entsprechende Umsetzung finden. So wurde oben bereits aufgezeigt, dass die Verwendung von Botnetzen von zahlreichen Straftatbeständen erfasst ist.[87] Auch das Abgreifen oder Verändern von Daten ist je nach Einzelfall typischerweise strafbar (§§ 202a, 202b, 303a StGB). Kommt es aufgrund des Zugriffs auf ein Informationssystem zu Störungen des Betriebs, greift bei bedeutsamen Datenverarbeitungen zudem § 303b StGB.

Andererseits lässt sich argumentieren, dass § 202a StGB den europäischen Vorgaben aufgrund seiner Schutzrichtung nicht genüge, indem er primär Daten schützt, wohingegen auf europäischer Ebene der Schutz von Systemen im Vordergrund steht.[88] Da der europarechtlich geforderte Schutz von Systemen nicht zwingend mit dem oben ausgeführten[89] Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität von IT-Systemen gleichzusetzen ist, lässt sich über die Frage, ob sich hieraus ein weiterer Umsetzungsbedarf durch deutsches Recht ergibt, sicher streiten. Von Bedeutung dürfte dabei allerdings sein, dass ein Zugriff auf ein System unter Überwindung von Sicherheitsmaßnahmen, ohne gleichzeitig einen Zugang zumindest zu Systemdaten zu erlangen, in tatsächlicher Hinsicht sehr selten sein wird, da sich Schadsoftware ohne Zugang zu Daten kaum für weitere (kriminelle) Handlungen nutzen lässt.[90] Außerdem dürfte sich argumentieren lassen, dass derartige Fallkonstellationen typischerweise kein größeres Gefahrenpotenzial aufweisen und daher unter die «leichten Fälle» fallen, für welche die europarechtlichen Vorgaben gerade keine zwingende Strafbarkeit vorschreiben. Mithin spricht vieles gegen eine Pflicht, § 202e StGB-E einzuführen, zumal dieser bei genauerer Betrachtung dieselbe Schutzrichtung hat, wie auch schon § 202a StGB.[91]

6. Praktische Umsetzung des § 202e StGB-E und Ergebnis

Die Untersuchung hat gezeigt, dass entgegen der Argumentation des aktuellen Gesetzentwurfs, die Einführung einer Strafvorschrift zum sog. «digitalen Hausfriedensbruch» nicht zwingend notwendig ist. Insbesondere be-

81 Richtlinie 2013/40/EU, ABl. EU L 218, 8.

82 Mavany, KriPoZ 2016, S. 106 (S. 108).

83 Vgl. Art. 2 Rahmenbeschluss 2005/222/JI des Rates vom 24. Februar 2005 über Angriffe auf Informationssysteme, ABl. EU L 69, 67; Art. 3 Richtlinie 2013/40/EU, ABl. EU L 218, 8; Art. 2 Übereinkommen des Europarats über Computerkriminalität, BGBl. 2008 II Nr. 30, 1242.

84 Erwägungsgründe 3 f. Richtlinie 2013/40/EU, ABl. EU L 218, 8.

85 Erwägungsgründe 5 f. Richtlinie 2013/40/EU, ABl. EU L 218, 8.

86 Vgl. bspw. zur Umsetzung der Cybercrime-Konvention in Deutschland und Österreich den Überblick bei Popp, Computerstrafrecht in Europa, MR-Int 2007, S. 48.

87 Siehe bereits oben Kapitel 3.1.

88 In diese Richtung etwa Gröseling/Höfinger, Hacking und Computerspionage, MMR 2007, S. 549 (S. 551); Gercke, Die Entwicklung des Internetstrafrechts im Jahr 2006, ZUM 2007, S. 282 (S. 282 f.).

89 Siehe bereits Kapitel 4.

90 Mavany, KriPoZ 2016, S. 106 (S. 109).

91 Vgl. zur Schutzrichtung bereits Kapitel 4 sowie ausführlich die Ausführungen bei Mavany, KriPoZ 2016, S. 106.

stehen keine gravierenden Strafbarkeitslücken und auch die Schutzrichtung des neu einzuführenden § 202e StGB-E unterscheidet sich im Ergebnis nicht von der des § 202a StGB. Allenfalls aufgrund europarechtlicher Vorgaben ließe sich die Notwendigkeit des § 202e StGB-E begründen. Letztlich sprechen allerdings, wie dargelegt, auch hier gute Gründe gegen eine solche Notwendigkeit.

Zu guter Letzt lassen sich auch noch einige praktische Gründe gegen die Einführung des § 202e StGB-E anführen. So wurde bereits von einigen Autoren darauf hingewiesen, dass Taten nach § 202e StGB-E u.a. aufgrund der Verwendung von Anonymisierungswerkzeugen und des regelmäßigen Auslandbezugs einschlägiger Sachverhalte, kaum verfolgt werden können.[92] Aus diesem Grund sei es zielführender, mittels Produkthaftung oder Anreizen bereits das Entstehen von Sicherheitslücken in Systemen einzudämmen.[93] Alles in allem ist die Schaffung eines neuen Straftatbestands zum digitalen Hausfriedensbruch daher abzulehnen.[94]

7. Literatur

Biselli, Anna, Digitaler Hausfriedensbruch: Hessen will neuen Straftatbestand gegen bereits illegale Botnetze einführen, netzpolitik.org, https://netzpolitik.org/2016/digitaler-hausfriedensbruch-hessen-will-neuen-straftatbestand-gegen-bereits-illegale-botnetze-einfuehren/.

Buermeyer, Ulf, «Digitaler Hausfriedensbruch»: IT-Strafrecht auf Abwegen, Legal Tribune Online, http://www.lto.de/recht/hintergruende/h/entwurf-straftatbestand-digitaler-hausfriedensbruch-botnetze-internet/.

Buermeyer, Ulf/Golla, Sebastian J., «Digitaler Hausfriedensbruch» – Der Entwurf eines Gesetzes zur Strafbarkeit der unbefugten Benutzung informationstechnischer Systeme, K&R, 2017, Heft 1, S. 14–18.

Eisele, Jörg, Computer- und Medienstrafrecht, C.H. Beck, München 2013.

Fischer, Thomas, Strafgesetzbuch mit Nebengesetzen, 64. Aufl., C.H. Beck, München 2017.

G DATA Software AG, Was ist eigentlich ein Botnet?, gdata.de, https://www.gdata.de/ratgeber/was-ist-eigentlich-ein-botnet.

Gercke, Marco, Die Entwicklung des Internetstrafrechts im Jahr 2006, ZUM, 2007, Heft 4, S. 282–294.

Graf, Jürgen-Peter, § 202a. In: Joecks, Wolfgang/Miebach, Klaus (Hrsg.), Münchener Kommentar zum StGB, 2. Aufl., C.H. Beck, München 2012.

Gröseling, Nadine/Höfinger, Frank Michael, Hacking und Computerspionage, Auswirkungen des 41, StÄndG zur Bekämpfung der Computerkriminalität, MMR, 2007, Heft 9, S. 549–553.

Heger, Martin, § 202a. In: Kühl, Kristian (Hrsg.), Strafgesetzbuch Kommentar, 28. Aufl., C.H. Beck, München 2014.

Lenckner, Theodor/Eisele, Jörg, § 202a. In: Schönke, Adolf/Schröder, Horst (Hrsg.), StGB, 29. Aufl., C.H. Beck, München 2014.

Malek, Klaus/Popp, Andreas, Strafsachen im Internet, 2. Aufl., C.F. Müller, Heidelberg 2015.

Mavany, Markus, Digitaler Hausfriedensbruch – Allheilmittel oder bittere Pille?, ZRP, 2016, Heft 8, S. 221–223.

Mavany, Markus, Pferde, Würmer, Roboter, Zombies und das Strafrecht? Vom Sinn und Unsinn neuer Gesetze gegen den sog. digitalen Hausfriedensbruch, KriPoZ, 2016, Heft 2, S. 106–112.

Popp, Andreas, Computerstrafrecht in Europa, Zur Umsetzung der «Convention on Cybercrime» in Deutschland und Österreich, MR-Int, 2007, Heft 2, S. 48–88.

Rengier, Rudolf, Strafrecht Besonderer Teil 2, 17. Aufl., C.H. Beck, München 2016.

Roos, Philipp/Schumacher, Philipp, Botnetze als Herausforderung für Recht und Gesellschaft, MMR, 2014, Heft 6, S. 377–383.

Wikipedia, Denial of Service, wikipedia.org, https://de.wikipedia.org/wiki/Denial_of_Service.

Wikipedia, Spam, wikipedia.org, https://de.wikipedia.org/wiki/Spam.

92 So bspw. Buermeyer, a.a.O.; Buermeyer/Golla, a.a.O., S. 16.

93 Buermeyer, a.a.O.

94 So auch schon Buermeyer, a.a.O.; Buermeyer/Golla, a.a.O.; Mavany, ZRP 2016, S. 221; Mavany, KriPoZ 2016, S. 106.