KriPoZ Kriminalpolitische Zeitschrift JuP

„Junges Publizieren“

Grundlagenseminararbeit von

Sophia Regina Weis

„Der digitale Hausfriedensbruch als Straftat“

Ludwig-Maximilians-Universität München
Prof. Dr. Mark Zöller

Abgabedatum: 5.10.2020

Inhaltsverzeichnis

I. Einleitung

Während die Digitalisierung es ermöglicht, sich immer schneller zu vernetzen und Daten auszutauschen, steigen auch im Bereich der digitalen Kriminalität (Cyberkriminalität) die Zahlen immer weiter an.
Große Identitätsdiebstähle wie Collection #1- #5[1], Hackerangriffe auf den deutschen Bundestag[2], massive Verbreitung von persönlichen Daten von Politikern und Prominenten[3] sowie Ransomeware-Angriffe auf Krankenhäuser[4] zeigen die Schattenseite der Digitalisierung auf.
Gerade im Hinblick auf solche Vorkommnisse wird die Thematik bezüglich der Bekämpfung von Cyberkriminalität immer präsenter. Dabei wird unter anderem darüber diskutiert, inwieweit das Strafrecht als „ultima-ratio" bereits Anwendung findet oder gegebenenfalls noch Anwendung finden muss. Insbesondere das Themengebiet des „digitalen Hausfriedensbruchs" steht dabei im Raum.

II. Der „digitaler Hausfriedensbruch"

Unter einem „digitalen Hausfriedensbruch" versteht man den unbefugten Zugang zu einem informationstechnischen System.
Dieser kann zum einen ohne eine Schadsoftware, beispielsweise durch die Eingabe eines zuvor erspähten Pins oder durch das Erlangen und anschließende Eindringen in ein nicht gesichertes System, erfolgen. Zum anderen erfolgt ein digitaler Hausfriedensbruch, vor allem im Bereich schwerwiegender Cyberkriminalität, durch den Einsatz einer Schadsoftware.
Von einem digitalen Hausfriedensbruch mittels einer Schadsoftware wird dann gesprochen, wenn die Schadsoftware auf dem System installiert wird, da bereits die reine Infiltration, also die Zugangserlangung zum System, ausreichend ist.[5]

1. Zugangserlangung mittels einer Schadsoftware

Um Zugang zu einem informationstechnischen System zu erlangen, muss zunächst das jeweilige Zielsystem mit einer Schadsoftware infiltriert werden. Dies kann auf verschiedene Weise erfolgen.
Neben der relativ seltenen Methode eine Schadsoftware direkt durch einen USB-Stick oder eine CD-ROM aufzuspielen, findet die Infektion durch eine im Anhang einer E-Mail oder als Teil einer Nachricht in einem sozialen Netzwerk befindliche Software häufiger Anwendung.[6]
Die derzeit gängigste Methode ist jedoch die sog. „Drive-by-Infektion". Dabei hackt der Täter eine Website und manipuliert diese so, dass durch das alleinige Aufrufen dieser Website die Schadsoftware automatisch im Hintergrund auf das System heruntergeladen wird.[7]

---

1 Abrufbar unter: https://www.pc-magazin.de/ratgeber/datenklau-aktuell-collection-1-betroffen-pruefen-have-i-been-pwned-3200357.html (zuletzt abgerufen am: 27.9.2020).
2 Bundesamt für Sicherheit in der Informationstechnik, Die Lage der IT-Sicherheit in Deutschland 2016, abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2016.html (zuletzt abgerufen am: 27.9.2020).
3 *Eisenkrämer*, Riesiges Datenleck bei Politikern und Prominenten, abrufbar unter: https://www.springerprofessional.de/internetkriminalitaet/datensicherheit/riesiges-datenleck-bei-politikern-und-prominenten/16374550 (zuletzt abgerufen am 10.9.2020).
4 Abrufbar unter: https://www.zdf.de/nachrichten/panorama/hacker-angriff-uniklinik-duesseldorf-100.html (zuletzt abgerufen am: 27.9.2020).
5 *Mavany,* KriPoZ 2016, 106 (108).
6 *Mavany,* KriPoZ 2016, 106 (107).
7 *Roos/Schumacher,* MMR 2014, 377 (378).

Nach den Angaben des Bundesamts für Sicherheit in der Informationstechnik werden nachweislich jeden Tag allein bis zu 110.000 Systeme mit einer sog. „Botnetz-Schadsoftware“ (Botware) infiziert.[8] Jedoch kann aufgrund der nicht entdeckten Infektionen von einer durchaus höheren Infektionsrate ausgegangen werden.
Botnetze stellen das zentrale Werkzeug des Täters, mithin die infrastrukturelle Grundlage von Cyberkriminalität, dar.[9]

2. Entstehung eines Botnetzes

Zuerst muss die sog. „Botware“ programmiert werden. Anschließend, in der zweiten Phase des sog. „Spreadings“, werden möglichst viele Systeme (Bots) mit der Botware in einer solchen Weise infiziert, dass diese auch einen Neustart überstehen kann. Dabei kommt als Bot jedes mit dem Internet ständig oder teilweise verbundene System in Betracht.[10] Neben Computern werden vermehrt auch mobile sowie sog. intelligente Endgeräte des Internet of Things (IoT) infiziert, wodurch diese auch Teil eines Botnetzes sein können.[11]
Somit wird der digitale Hausfriedensbruch im Zusammenhang mit Botnetzen in der Phase des „Spreadings“ verwirklicht.[12]
In einer dritten Phase verbinden sich dann die einzelnen Bots über das Internet mit dem zentralen „Command and Control-Server“ (CC-Server), welcher vom sog. „Botmaster“ ferngesteuert und für kriminelle Zwecke missbrauchen werden kann, ohne dass der eigentliche Nutzer dies bemerkt.[13] Da die „Bots“ die über den CC- Server vom Botmaster erteilten Befehle blind ausführen, werden diese als „Zombie“ und das zusammengeschlossene Botnetz selbst als „Zombie-Armee“ bezeichnet.[14]

3. Nutzungsmöglichkeiten eines Botnetzes

Auch wenn es in letzter Zeit gelungen ist, große Botnetze wie „Avalanche“ und „Andromeda“ zu zerschlagen, spielen Botnetze in der Cyberkriminalität aufgrund ihrer vielfältigen Nutzungsmöglichkeiten weiterhin eine zentrale Rolle.[15]
Darunter fällt beispielsweise die Möglichkeit des Spam-Mail-Versands[16], aber auch das Ausspähen und Kopieren von (persönlichen) Daten oder die Verbreitung einer Ransomware bis hin zum Betrug im Online-Banking und dem „Bitcoin-Mining“[17] ist durch den Einsatz eines Botnetzes möglich.[18]
Vor allem aber werden Botnetze zur Ausübung von „Distributed-Denial-of-Service-Attacken (DDoS-Attacken) genutzt, die zu den größten Gefährdungen im Cyberraum zählen.[19]

---

8 Bundesamt für Sicherheit in der Informationstechnik, BSI-Magazin 2019, „Mit Sicherheit – IT-Grundschutz als Fundament für Informationssicherheit“, abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Magazin/BSI-Magazin_2019_02.pdf?__blob=publicationFile&v=6 (zuletzt abgerufen am 26.9.2020).
9 *Mavany,* KriPoZ 2016, 106 (107).
10 BT-Drs. 19/1716, S. 1.
11 BKA-Cybercrime, Bundeslagebild 2018, abrufbar unter: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2018.html;jsessionid=F293BBB6E2C2D5A62651D10296BAA05F.live2292?nn=28110 (zuletzt abgerufen am 26.9.2020).
12 *Mavany,* KriPoZ 2016, 106 (108).
13 *Mavany,* KriPoZ 2016, 106 (107).
14 *Kahler/Hoffmann-Holland,* KriPoZ 2018, 267 (270); *Mavany,* KriPoZ 2016, 106 (107).
15 *Roos/Schumacher,* MMR 2014, 377 (378).
16 *Roos/Schumacher,* MMR 2014, 337 (378).
17 *Heine,* NStZ 2016, 441 (442).
18 *Roos/Schumacher,* MMR 2014, 377 (378).
19 *Roos/Schumacher,* MMR 2014, 377 (378).

Dabei werden massive Datenanfragen an einen ausgewählte Server gestellt, um diesen unter der großen Anfragelast „zusammenbrechen“ zu lassen und somit die dort bereitgestellten Dienste zu stören oder sogar ganz zu eliminieren.[20]
Aufgrund seiner Größe von bis zu 9 Millionen Bots und seiner vielseitigen Einsetzungsmöglichkeiten galt das Necurs-Botnetz bis 2020 als eines der gefährlichsten Botnetze der Welt.[21]
Auch stellt die Möglichkeit des „Cybercrime-as-a-Service“, bei welchem Cyberkriminelle ihre Dienste oder die Nutzung, beispielsweise eines Botnetzes, gegen Bezahlung anbieten, eine zusätzliche Bedrohung im Cyberraum dar, da es dadurch jedermann ermöglicht wird das kriminelle „Know-How“ zu erwerben.[22]

III. Vorhandener strafrechtlicher Schutz des digitalen Hausfriedensbuchs

Nicht nur Privatpersonen, sondern vor allem auch Unternehmen und kritische Infrastrukturen (KRITIS) sind von Botnetz-Angriffen, mithin auch von „digitalen Hausfriedensbrüchen“ betroffen. Demnach stellt sich die Frage, inwieweit ein strafrechtlicher Schutz bereits existiert.

1. Strafrechtlicher Schutz nach dem Strafgesetzbuch und deren Strafbarkeitslücken

a) § 202a StGB – Ausspähen von Daten

aa) Straftatbestand des § 202a StGB

Zunächst kommt bei der Infiltration einer Schadsoftware, durch die ein digitaler Hausfriedensbruch verwirklicht wird, eine Strafbarkeit nach § 202a StGB in Betracht.
Voraussetzung hierfür ist, dass der Täter sich oder einem Dritten Zugang zu Daten, die nicht für ihn bestimmt sind und gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung, verschafft.[23] Geschützt ist nach herrschender Ansicht die formelle Verfügungsbefugnis des Berechtigten hinsichtlich der in den Daten enthaltenen Informationen.[24]
Unter dem Begriff der Daten versteht man alle durch Zeichen oder kontinuierliche Funktionen dargestellte Informationen, die sich als Gegenstand oder Mittel der Datenverarbeitung für eine Datenverarbeitungsanlage codieren lassen oder die das Ergebnis eines Datenverarbeitungsvorgangs darstellen.[25] Unter den weiten Datenbegriff fallen auch Programmdaten, da diese aus einer Vielzahl von Daten zusammengefügt sind.[26] § 202a Abs. 2 StGB schränkt den Datenbegriff dahingehend ein, dass nur solche Daten in Betracht kommen, welche nicht unmittelbar wahrnehmbar sind und zudem gespeichert oder übermittelt werden können.[27]
Eine Strafbarkeit nach § 202a StGB kommt somit nur dann in Betracht, wenn der Dateninhaber zum einen durch eine mechanische oder technische Zugangssicherung sein Interesse an der Geheinhaltung der Daten zum Ausdruck

[20] *LG Düsseldorf*, MMR 2011, 624 (625).
[21] *Tom Burt*, New action to disrupt world’s largest online criminal network, abrufbar unter: https://blogs.microsoft.com/on-the-issues/2020/03/10/necurs-botnet-cyber-crime-disrupt/ (zuletzt abgerufen am 27.9.2020).
[22] *Roos/Schumacher* MMR 2014, 377 (380 f.).
[23] *Eisele*, in Schönke/Schröder, StGB, 30. Auflage (2019), § 202a Rn. 7.
[24] *Weidemann*, in BeckOK-StGB, 47. Ed. (Stand: 1.8.2020), § 202a Rn. 2; *Hassemer*, in Auer-Reinsdorff/Conrad, Handbuch IT- und Datenschutzrecht, 3. Auflage (2019), S. 2672 Rn. 80.
[25] *Eisele*, in Schönke/Schröder, StGB, § 202a Rn. 3.
[26] *Eisele/Nolte,* CR 2020, 488 (498).
[27] *Eisele*, in Schönke/Schröder, StGB, § 202a Rn. 4.

gebracht hat und diese durch den Täter überwunden worden ist.[28] Eine solche Zugangssicherung liegt dann vor, wenn sie objektiv geeignet und subjektiv gewollt ist, Dritte vom Zugriff auf die Daten auszuschließen oder den Zugang wenigstens nicht unerheblich zu erschweren, beispielsweise durch die Vergabe von Passwörtern, der Benutzung von Tastaturschlössern und Antivirensoftware.[29]

Zum anderen ist es nach § 202a StGB nötig, dass der Täter mit der Infiltration der Schadsoftware auf die gespeicherten oder übermittelten Daten des Zielsystems zugreifen könnte. Die bloße Zugangsmöglichkeit zu den Daten des befallenen Systems ist demnach ausreichend. Ein tatsächliches Ausspähen oder eine Besitzerlangung muss nicht stattgefunden haben,[30] wodurch § 202a StGB das Hacking strafrechtlich erfasst.[31]

bb) Strafbarkeitslücken des § 202a StGB in Bezug auf den digitalen Hausfriedensbruch

Nach dem Wortlaut des § 202a StGB ist allein die Zugangsverschaffung zu Daten unter Strafe gestellt. Der digitale Hausfriedensbruch ist jedoch nicht erst mit der Möglichkeit der Kenntnisnahme von Daten, sondern bereits mit dem alleinigen unbefugten Zugang zu einem informationstechnischen System gegeben.

Eine Strafbarkeitslücke bezüglich § 202a StGB kommt demnach dann in Betracht, wenn der Täter zwar Zugang zu dem IT-System erlangt, jedoch nicht die Möglichkeit hat, auf gespeicherte Daten zuzugreifen.[32]

In der technischen Realität erscheint diese juristische Strafbarkeitslücke jedoch so gut wie nicht vorhanden zu sein, da beispielsweise eine Botware, die nicht auch in der Lage ist, einen Zugang, zu den auf dem Zielsystem gesicherten Daten zu verschaffen, dem Botmaster kaum nützlich sein wird, da üblicherweise die Daten des Betroffenen für weitere Straftaten erforderlich sind.[33]

Eine Konstellation, in der der Täter durch die Infiltration einer Schadsoftware nicht auch die Möglichkeit der Kenntnisnahme der auf dem IT-System befindlichen Daten erlangt, scheint somit kaum vorstellbar, weshalb bei einem digitalen Hausfriedensbruch regelmäßig § 202a StGB verwirklicht wird.[34]

Aufgrund dessen, wird in der Literatur § 202a StGB bereits als „elektronischer Hausfriedensbruch" bezeichnet.[35]

Jedoch bleibt einem Betroffenen der strafrechtliche Schutz des § 202a StGB dann verwehrt, wenn keine oder eine nach § 202a StGB unzureichende Zugangssicherung der Daten vorliegt, da der Täter dann entweder keine Zugangssicherung zu überwinden hat oder ihm dies nicht ausreichend erschwert worden ist. Somit hängt ein strafrechtlicher Schutz unter anderem von den technischen Fähigkeiten jedes einzelnen Nutzers ab.

Insbesondere im wirtschaftlichen Bereich kann zwar von ausreichenden Zugangssicherungen ausgegangen werden, da insbesondere im Bereich kritischer Infrastrukturen durch das IT-Sicherheitsgesetz IT-Mindeststandards zur Sicherung von informationstechnischen Systemen, mithin der darauf vorhandenen Daten, vorgeschrieben werden,[36] jedoch sind insbesondere im privaten Bereich nicht ausreichende Zugangssicherungen vorhanden[37], sodass in diesen Fällen ein strafrechtlicher Schutz des § 202a StGB nicht eingreift.

---

28 *Bär*, in Wabnitz/Janovsky/Schmit, Handbuch Wirtschafts- und Steuerrecht, 5. Auflage (2020), 5. Kapitel Rn. 72; *Stömer*, Online-Recht: Juristische Probleme der Internet-Praxis erkennen und vermeiden, 4. Auflage (2006), S. 450; *Marberth-Kubicki*, Computer – und Internetstrafrecht, 2. Auflage (2010), Rn. 88.

29 *Roos/Schumacher*, MMR 2014, 337 (379); *Eisele,* Jura 2012, 922 (925); *Eisele*, Computer- und Medienstrafrecht, 2013, Kapitel 4 § 6 Rn. 15.

30 *Graf,* in: MüKo-StGB, 3. Auflage (2017), § 202a Rn. 62; *Marberth-Kubicki*, Rn. 95; *Eisele*, Jura 2012, 992 (925).

31 *Ernst,* NJW 2007, 2661 (2661).

32 *Eisele/Nolte,* CR 2020, 488 (489).

33 *Mavany,* KriPoZ 2016, 106 (109).

34 *Buermeyer/Golla,* K&R 2017, 14 (15).

35 *Mavany,* KriPoZ 2016, 106 (109); *Golla/Mühlen*, Russen-Hacker und Zombie-Rechner: Gesetzesentwurf zu digitalem Hausfriedensbruch, abrufbar unter: https://www.telemedicus.info/russen-hacker-und-zombie-rechner-gesetzesentwurf-zu-digitalem-hausfriedensbruch/ (zuletzt abgerufen am: 25.8.2020); *Buermeyer/Golla*, K&R 2017, 14 (15); *Marberth-Kubicki*, Rn. 84.

36 § 8a I 1 ITSichG, *Oehmichen/Weißenberger,* KriPoZ 2019, 174 (174 f.).

37 BVerfGE 120, 274 (306); BT-Drs. 19/1716, S. 3; *Marbeth-Kubicki,* Rn. 117; *Malek/Popp,* Strafsachen im Internet, 2. Auflage (2015), Rn. 169.

b) § 202b StGB – Abfangen von Daten

Auch kann die Infiltration einer Schadsoftware nach § 202b StGB strafbar sein.
Nach § 202b StGB macht sich strafbar, wer unbefugt sich oder einem anderen unter Anwendung von technischen Mitteln nicht für ihn bestimmte Daten aus einer nichtöffentlichen Datenübermittlung verschafft. Demnach kann § 202b StGB dann erfüllt sein, wenn der Täter die Infiltration durch Zugriff auf eine Datenübermittlung vornimmt. Dies ist beispielsweise dann gegeben, wenn der Täter alle ein- und ausgehenden E-Mails abfängt und diese mit schadhaftem Anhang weiterleitet.[38]

c) § 303a StGB – Datenveränderung

aa) Straftatbestand des § 303a StGB
In den meisten Fällen kommt bei der Infiltration mit einer Schadsoftware jedoch eine Strafbarkeit gemäß § 303 StGB in Betracht.
Nach § 303a StGB macht sich strafbar, wer rechtswidrig Daten löscht, unterdrückt, unbrauchbar macht oder verändert.[39] Dadurch wird das Interesse des Verfügungsberechtigten an der unversehrten Verwendbarkeit, der in den gespeicherten Daten enthaltenen Informationen, geschützt.[40]
In Bezug auf die Infiltration einer Schadsoftware kann eine Strafbarkeit aufgrund einer Veränderung von Daten einschlägig sein. Verändert werden Daten, wenn sie, wenn auch nur vorübergehend, einen anderen Informationsgehalt erhalten und dadurch ihr Aussagewert inhaltlich umgestaltet wird.[41]
Das Aufspielen einer Schadsoftware müsste somit, um den Tatbestand des § 303a StGB zu erfüllen, den Informationsgehalt anderer, bereits vorhandener Daten verändern.[42]
Dabei ist im Folgenden zu differenzieren, auf welches Betriebssystem die Schadsoftware infiltriert wird.
Ist das Betriebssystemen eine einzige Programmdatei, so wird durch jedes neue Aufspielen eines Programms dieses insgesamt verändert.[43] Dies ist unter anderem bei Unix-ähnlichen Programmen wie macOS oder Linux der Fall, bei dem das Betriebssystem als ein hierarchisches Verzeichnis mit beliebigen Unterverzeichnissen organisiert ist.[44] Nach dem Grundprinzip „Alles ist eine Datei“, bedeutet jedes „Hinzufügen“, mithin auch das einer Schadsoftware, einen zusätzlichen Eintrag in das Verzeichnis und führt dadurch zu einer Veränderung des Betriebssystems insgesamt.[45] Der Tatbestand der Datenveränderung gemäß § 303a StGB ist somit mit der Installation der Schadsoftware erfüllt.
Anders verhält es sich jedoch beispielsweise bei Betriebssystemen wie Windows, die über eine sog. „Registry“ verfügen. Diese ist nicht Teil des eigentlichen Programms, sondern stellt die zentrale hierarchische Konfigurationsdatenbank dar, auf welcher alle systemrelevanten Informationen für Windows und installierte Programme hinterlegt und abgerufen werden können.[46]
Durch das „Hinzufügen“ eines weiteren Eintrags in eine Datenbank beispielsweise durch die Installation einer

38 *Mavany,* KriPoZ 2016, 106 (109).
39 *Wieck-Noodt,* in: MüKo-StGB, 3. Auflage (2019), § 303a Rn. 11.
40 *Wieck-Noodt,* in: MüKo-StGB, § 303a Rn 2; *Zaczyk*, in: Kindhäuser/Neumann/Paeffgen, StGB, 29. Auflage (2018), § 303a Rn. 2; *Ernst,* NJW 2003, 3233 (3237); *Eisele*, Kapitel 4 § 6 Rn. 62.
41 *Marberth-Kubicki*, Rn. 142.
42 *Marberth-Kubicki,* Rn. 142.
43 *Heine,* NStZ 2016, 441 (443).
44 *Heine,* NStZ 2016, 441 (443).
45 *Heine,* NStZ 2016, 441 (443).
46 *Heine,* NStZ 2016, 441 (443).

(Schad)-Software, werden jedoch bereits vorhandenen Daten oder Computerprogramme nicht in ihrem Aussagewert verändert, sondern lediglich die Datenbank in ihrer Gesamtheit vergrößert, weshalb der Tatbestand des § 303a StGB dann nicht verwirklicht ist.[47]
Jedoch kann eine Datenveränderung im Sinne des § 303a StGB dann angenommen werden, wenn die Schadsoftware, insbesondere eine Botware, so auf dem Zielsystem installiert wird, dass diese einen Neustart übersteht, da dies nicht ohne die Veränderung der entsprechenden Systemsteuerdateien möglich ist.[48]

bb) Strafbarkeitslücken des § 303a StGB in Bezug auf den digitalen Hausfriedensbruch
Eine Strafbarkeitslücke nach § 303a StGB besteht somit dann, wenn das Hinzufügen der Schadsoftware keine Datenveränderung herbeiführt, weil das Betriebssystem auf eine Datenbank zurückgreift und die Software nicht in einer solchen Weise auf das System installiert wird, dass diese einen Neustart überstehen soll.
Jedoch ist eine Schadsoftware, die nicht auch einen Neustart zu überstehen vermag, für den Täter nur von geringem Nutzen.

2. Schutz nach datenschutzrechtlicher Strafvorschrift § 42 BDSG

Über das materielle Kernstrafrecht hinaus, käme ein Schutz nach § 42 BDSG (i.V.m. Art. 84 DSGVO) in Betracht. Jedoch ist bereits der persönliche Anwendungsbereich dieser Norm strittig. Einer Auffassung nach ist die Norm auf jeden anwendbar, da der Wortlaut keine Beschränkungen hinsichtlich bestimmter Tätergruppen vornimmt.[49]
Die Gegenansicht nimmt im Hinblick auf den Bestimmtheitsgrundsatz an, dass die Norm nur für die Personen gilt, die die Regelungen des BDSG zu befolgen haben, mithin Verantwortliche (Art. 4 Nr. 7 DSGVO) bzw. Auftragsverarbeiter (Art. 4 Nr. 8 DSGVO) öffentlicher (§ 2 Abs. 1-3 BDDG) bzw. nichtöffentlicher (§ 2 Abs. 4, 5 BDSG) Stellen.
Da das Gesetz sich jedoch auf die Verarbeitung personenbezogener Daten bezieht, ist es nicht primär für die Strafbarkeit eines digitalen Hausfriedensbruchs heranzuziehen.

IV. Vorschläge zur „Lückenschließung“ im Bereich des digitalen Hausfriedensbruchs

1. Gesetzesentwurf des § 202e StGB

a) Zielsetzung und Notwendigkeit des Gesetzesentwurfs

Insbesondere im Zusammenhang mit der Botnetz-Kriminalität hat der Bundesrat in der 19. Wahlperiode einen vom Land Hessen ursprünglich eingebrachten und zuvor dem Diskontinuitätsprinzip zum Opfer gefallenen wortlautidentischen Gesetzesentwurf in den Bundestag eingebracht.[50]
Dieser soll, durch die Einführung eines neuen Straftatbestandes § 202e StGB, die unbefugte Benutzung informationstechnischer Systeme unter Strafe stellen, um einen erweiterten strafrechtlichen Schutz des Grundrechts auf

47 *Heine,* NStZ 2016, 441 (443).
48 *Eichelberger,* MMR 2004, 594 (595); *Heine,* NStZ 2016, 441 (443).
49 *Eisele/Nolte,* CR 2020, 488 (493).
50 BT-Drs. 19/1716.

Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (IT-Grundrecht) gewährleisten zu können.[51]

Insbesondere sollte eine bessere Bekämpfung der Botnetz-Kriminalität ermöglicht werden, da durch die Verwendung derer weitreichende Rückschlüsse auf die Persönlichkeit, bis hin in den Kernbereich höchstpersönlicher Lebensgestaltung, möglich sind.[52] Es sei die Aufgabe des Strafrechts, den lückenlosen Schutz des IT- Grundrechts sicherzustellen insbesondere, da sich der Einzelne nicht ausreichend gegen eine Infiltration seines Computers mit einer Schadsoftware, mithin gegen eine unbefugte Benutzung seines Systems schützen könne.[53]

Darüber hinaus würde dem Ziel der vollständigen Umsetzung des Art. 2 des Budapester Übereinkommens über Computerkriminalität[54] und des Art. 3 der EU-Richtlinie über Angriffe auf Informationssysteme[55] nachgegangen werden. Dort heißt es in beiden Vorschriften, dass jeder Vertragspartei bzw. jeder Mitgliedsstaat erforderliche Maßnahmen zu treffen hat, um den unbefugten Zugang zu einem Informationssystem als Ganzes oder zum Teil unter Strafe zu stellen.

Der Gesetzesbegründung nach wären die bereits bestehenden Straftatbestände nicht für die Durchsetzung dieser Ziele ausreichend, da insb. § 202a StGB, § 303a StGB und § 303b StGB nur bestimmte Daten, nicht aber das technische System als solches schützen.[56] Schon das ausschließliche Gebrauchsrecht des rechtmäßigen Nutzers sei schützenswert.[57]

Aufgrund dessen sollen die Rechtsgedanken der § 123 StGB und § 248b StGB in die digitale Welt übertragen und dadurch der neue Straftatbestand des § 202e StGB geschaffen werden.[58]

b) Der neue Straftatbestand des § 202e StGB

Der durch den Bundesrat eingebrachte Gesetzesentwurf § 202e StGB - Unbefugte Benutzung informationstechnischer Systeme - soll nach den Angaben des § 202d StGB in das Strafgesetzbuch mit folgendem Inhalt eingefügt werden:

„ (1) Wer unbefugt

1. sich oder einem Dritten den Zugang zu einem informationstechnischen System verschafft,
2. ein informationstechnisches System in Gebrauch nimmt oder
3. einen Datenverarbeitungsvorgang oder einen informationstechnischen Ablauf auf einem informationstechnischen System beeinflusst oder in Gang setzt,

wird mit Geldstrafe oder Freiheitsstrafe bis zu einem Jahr bestraft, wenn die Tat nicht in anderen Vorschriften mit schwererer Strafe bedroht ist. Die Tat nach Satz 1 ist nur strafbar, wenn sie geeignet ist, berechtigte Interessen eines anderen zu beeinträchtigen.“[59]

In den folgenden sechs Absätzen werden Qualifikationen, besonders schwere Fälle, eine Versuchsstrafbarkeit, Begriffsdefinitionen und Antragserfordernisse normiert.

[51] BT-Drs. 19/1716, S. 3, 5.
[52] BT-Drs. 19/1716, S. 3; *Winkelmeier-Becker,* R&P 2019, 181 (182).
[53] BT-Drs. 19/1716, S. 3.
[54] Übereinkommen über Computerkriminalität vom 23.11.2001, Sammlung Europäischer Verträge (SEV) - Nr. 185, Artikel 2.
[55] Richtlinie 2013/40/EU des Europäischen Parlaments und Rates vom 12.8.2013 über Angriffe auf Informationssysteme zur Erlassung eines Rahmenbeschlusses 2005/222/JI des Rates, ABl. EU L 218, S. 8.
[56] BT-Drs. 19/1716, S. 11.
[57] BT-Drs. 19/1716, S. 11.
[58] BT-Drs. 19/1716, S. 5.
[59] BT-Drs. 19/1716, S. 9.

c) Kritische Stellungnahme

Grundsätzlich ist dem Ziel des Gesetzesentwurfes, den strafrechtlichen Schutz des IT-Grundrechts zu erweitern und die Botnetz-Kriminalität effektiver bekämpfen zu wollen, zuzustimmen.
Jedoch ist im Hinblick auf das „Ultima-ratio-Prinzip" des Strafrechts eine kritische Betrachtung dahingehend nötig, ob der „digitale Hausfriedensbruch", wie ihn § 202e StGB normiert, in dieser Art und Weise zielführend ist.

aa) Übertragung der Rechtsgedanken der §§ 123, 248b StGB
Allein die Übertragung der Rechtsgedanken der §§ 123, 248b StGB in die virtuelle Welt lässt sich nicht ohne weiteres, wie es der Gesetzesvorschlag annimmt, konstruieren.
Nach § 123 StGB wird das Hausrecht, das heißt die Freiheit zu bestimmen wer sich innerhalb einer bestimmten räumlichen Sphäre aufhalten darf und wer nicht, geschützt.[60]
Allein diesbezüglich ist auffällig, dass die Tathandlung des § 123 StGB das „widerrechtliche Eindringen" und nicht die „unbefugte Benutzung" ist, weshalb die Bezeichnung des „digitalen Hausfriedensbruchs" nicht zu der Normüberschrift der „unbefugten Benutzung informationstechnischer Systeme" passt.[61]
Überträgt man dennoch § 123 StGB in die digitale Welt, so müsste zunächst die Sphäre des „digitalen Hauses" zu bestimmen sein. Dies ist jedoch in technischer Hinsicht aufgrund der flächendeckenden Vernetzung und dem Nutzen von Clouds nicht genau möglich[62] und wäre mit dem Bestimmtheitsgrundsatz nicht vereinbar.
Auch ist es weiterhin fraglich, was das „virtuelle Hausrecht" genau umfasst[63] und wem dieses Recht zustehen soll, da Eigentümer, Nutzer und Dateninhaber unterschiedliche Personen sein können; man denke an einen geleasten, vermieteten oder unter Eigentumsvorbehalt verkauften Computer.[64]
Auch überzeugt die Übertragung des Rechtsgedanken der Ausnahmevorschrift des § 248b StGB in die virtuelle Welt nicht. Während in § 248b StGB der Eigentümer, welcher vor einer unbefugten Ingebrauchnahme geschützt werden soll,[65] bei einer Gebrauchsanmaßung vollständig um seine Nutzungsmöglichkeit gebracht wird, wird es der Berechtigte eines IT-Systems während einer „virtuellen Gebrauchsanmaßung" meist nicht. [66] Der „Betroffene" kann das System für seine Zwecke weiterhin nutzen und bekommt von alledem meist nichts mit, sodass die Gebrauchsanmaßung unterhalb der strafrechtlichen Erheblichkeitsschwelle läge.[67]
Der Schutz einer unbefugten Benutzung informationstechnischer Systeme durch die Übertragung der Rechtsgedanken der §§ 123, 248b StGB zu kreieren, geht somit an der technischen Realität vorbei.

bb) Schutzgut
Laut der Gesetzesbegründung soll das Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme das Schutzgut des § 202e StGB sein. Dieses Grundrecht wurde vom Bundesverfassungsgericht in seiner Entscheidung zur „Online-Durchsuchung" aus dem allgemeinen Persönlichkeitsrecht (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) hergeleitet.[68]

60 *Heger*, in: Lackner/Kühl, StGB, 29. Auflage (2018), § 123 Rn. 1.; *Schäfer,* in: MüKo-StGB, § 123 Rn. 2; *Tassi,* DuD 2017, 175 (177).
61 *Kahler/Hoffmannn-Holland,* KriPoZ 2018, 267 (268).
62 *Mavany,* KriPoZ 2016, 106 (110).
63 *Tassi*, DuD 2017, 175 (177 f.).
64 *Mavany,* KriPoZ 2016, 106 (110).
65 *Hohmann,* in: MüKo-StGB, § 248 b Rn. 1.
66 *Kahler/Hoffmannn-Holland,* KriPoZ 2018, 267 (268).
67 *Mavany,* ZRP 2016, 221 (222).
68 BVerfGE 120, 274 (313); BT-Drs. 19/1716 S. 11.

Nach dem *BVerfG* schützt das IT-Grundrecht das Interesse des Nutzers, dass die von den vom Schutzbereich erfassten informationstechnischen Systeme erzeugten, verarbeiteten und gespeicherten Daten vertraulich bleiben. Dies soll dadurch gewährleistet werden, dass nicht auf ein IT-System zugegriffen werden darf, wenn hierfür keine Berechtigung vorliegt.[69]

Die Integrität der informationstechnischen Systeme ist nur deshalb gefährdet, weil durch deren Verletzung letztendlich der Zugriff auf die in dem System gespeicherten Daten möglich ist.[70]

Bei der Gefährdung des IT-Systems handelt sich somit um eine „Annex-Gefahr"[71]. Das IT-Grundrecht schützt somit nicht primär das System selbst oder dessen unbeeinflussten Gebrauch, sondern stellt vielmehr eine Form des „vorgezogenen Datenschutzes" dar, welcher jedoch bereits durch die §§ 202a, 202b, 303a, 303b StGB sichergestellt wird.[72]

Das Grundrecht somit primär als Schutzgut einer Norm zur Bekämpfung des digitalen Hausfriedenbruch zu postulieren, überzeugt demnach nicht.

cc) Ausufernd weite Strafbarkeit

Darüber hinaus ist der Tatbestand des § 202e StGB durch die nahezu vollständige Einbeziehung aller IT-Systeme uferlos und entspricht nicht dem verfassungsrechtlichen Schutzgut des Grundrechts, welches dem Gesetzesentwurf zugrunde gelegt worden ist.

Verfassungsrechtlich geschützt werden allein solche IT-Systeme, die personenbezogene Daten des Betroffenen in einem solchen Umfang enthalten können, dass sie im Falle eines Eingriffs einen Einblick in wesentliche Lebensgestaltung der Person oder gar ein aussagekräftiges Bild der Persönlichkeit ermöglichen können.[73]

Die umfassende Einbeziehung hätte zur Folge, dass nahezu jede unbefugte Benutzung eines IT-Systems den objektiven Tatbestand des § 202e StGB erfüllt und somit auch alltägliche Handlungsweisen unter Strafe gestellt werden würden, wodurch die Grenzen des Übermaßverbotes gesprengt zu werden drohen.[74]

Auch vermag die in Abs. 1 S. 2 eingefügte Geringfügigkeitsklausel den Tatbestand nicht einzuschränken, da der Gesetzesbegründung nach ein „berechtigtes Interesse" wiederum nahezu jedes Interesse des Nutzers und sogar der Allgemeinheit darstellen kann.[75]

Somit geht die Einbeziehung nahezu aller IT-Systeme weit über den verfassungsrechtlichen Schutz hinaus, wodurch § 202e StGB strafrechtlich mehr schützen wollen würde, als verfassungsrechtlich vorgesehen ist.[76]

dd) Zwischenfeststellung

Aufgrund der aufgezeigten Unstimmigkeiten innerhalb des Tatbestandes und der Gesetzesbegründung ist der Tatbestand nicht zur gezielten Bekämpfung des digitalen Hausfriedensbruchs heranziehen und deswegen in seiner jetzigen Fassung abzulehnen.

69 BVerfGE 120, 274 (314).
70 *Eifert*, NVwZ 2008, 521 (522).
71 *Eifert,* NVwZ 2008, 521 (522).
72 *Mavany,* ZRP 2016, 221 (222); *Mavany,* KriPoZ 2016, 106 (112).
73 BVerfGE 120, 274 (314).
74 *Buermeyer/Golla,* K&R 2017, 14 (17); *Kahler/Hoffmannn-Holland,* KriPoZ 2018, 267 (275)*; Graf,* in: MüKo-StGB, § 202 a Rn. 8; *Basar,* JurisPR-StrafR 2016, IV. Bewertung und Ausblick, abrufbar unter: https://www.strafrecht.de/media/files/docs/180227_Basar_digitaler_Hausfriedensbruch_jurisPR-StrafR_26_2016.pdf (zuletzt abgerufen am: 15.9.2020).
75 BT-Drs. 19/1716, S. 16.
76 *Kahler/Hoffmannn-Holland,* KriPoZ 2018, 267 (269).

2. Ein Entwurf von Buermeyer/ Golla zur „Lückenschließung"

a) Der Entwurf

Ein Entwurf der Literatur möchte gezielt die Infektion mit einer Schadsoftware unter Strafe zu stellen. Nach *Dr. U. Buermeyer* und *Br. S. J. Golla* wäre die Ergänzung des § 202c Abs. 1 StGB um einen zweien Satz zielführend, welcher wie folgt lauten solle:
„Ebenso wird bestraft, wer eine Straftat vorbereitet, indem er einen Programmcode auf ein informationstechnisches System ohne Einwilligung einer berechtigten Person in der Absicht aufbringt, diesen ausführen zu lassen."[77]

b) Kritische Stellungnahme

Grundsätzlich ist der Idee, gezielt die Infektion eines IT-Systems mit einer Schadsoftware strafrechtlich unter Strafe stellen zu wollen, zuzustimmen. Jedoch berücksichtigt der Vorschlag nicht, dass die Absicht eines Hackers nicht zwingend in der Vorbereitung einer Straftat liegen muss.[78]
Es sollte allein das Eindringen in das IT-System mittels einer Schadsoftware unter Strafe gestellt werden. Dies an die Absicht zu knüpfen, den Programmcode auch ausführen zu lassen, ist in Bezug darauf, die bloße Installation einer Schadsoftware, mithin den digitalen Hausfriedensbruch unter Strafe stellen zu wollen, ein zu einschränkendes Kriterium.

3. Entwurf von Eisele/Nolte zur „Lückenschließung"

a) In Bezug auf § 202a StGB

Ein anderer Vorschlag in der Literatur, um die vorhandenen Lücken des § 202a StGB zu schließen und eine umfassende Strafbarkeit zu ermöglichen, wird von Eisele und Nolte wie folgt formuliert:
„(1) Wer unbefugt sich oder einem Dritten Zugang zu nicht für ihn bestimmte Daten oder Informationssystemen, die gegen unberechtigten Zugang besonders gesichert sind
1. unter Überwindung der Zugangssicherung oder
2. unter Verwendung unbefugt erlangter Passwörter oder sonstiger Sicherheitscodes oder
3. unter Ausnutzung eines von einem Dritten unbefugt geschaffenen Zugangs
verschafft
wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft."[79]
In den folgenden 4 Absätzen werden zudem die unbefugte Datenverschaffung, der Versuch und die Qualifikationen der Straftat nach Absatz 1 normiert.

77 *Buermeyer/Golla,* K&R 2017, 14 (18).
78 *Kahler/Hoffmann-Holland,* KriPoZ 2018, 267 (272).
79 *Eisele/Nolte,* CR 2020, 488 (491).

b) Kritische Stellungnahme

Zuzustimmen ist dem Vorschlag dahingehend, dass nunmehr der bloße Zugang zu einem informationstechnischen System unter Strafe gestellt wird, mithin der digitale Hausfriedensbruch mittels einer Schadsoftware. Durch Abs. 1 Nr. 2 wäre es unter anderem möglich, Fälle des „Phishings“[80] strafrechtlich eindeutig zu erfassen.[81] Durch die Einführung der Nr. 3 könnten zudem sogenannte „Backdoor[82] -Fälle“ erfasst werden.[83]
Auch die in Abs. 4 des Vorschlags genannte Versuchsstrafbarkeit ist zu befürworten. Denn bis dato ist zwar die Vollendung gem. § 202a StGB und die Vorbereitungshandlung gem. § 202c StGB unter Strafe gestellt, nicht jedoch das unmittelbare Ansetzen zur Tat, welches häufig jedoch allein von technischen Einzelheiten und Fähigkeiten des Täters abhängt.[84]
Jedoch wäre es unter anderem auch im Hinblick auf das Grundrecht auf Integrität und Vertraulichkeit informationstechnischer Systeme erstrebenswert, den alleinigen Zugriff auf ein informationstechnisches System, das speziell dazu geeignet ist, tiefe Einblick in persönliche Teile der Lebensgestaltung geben zu können, unter Strafe zu stellen, ohne dass hierbei eine Zugangssicherung bestehen und überwunden werden muss.
Ein weiterer Tatbestand könnte somit wie folgt lauten:
– Wer sich unbefugt Zugang zu einem informationstechnischen System verschafft, welches personenbezogene Daten enthält, die dazu geeignet sind, wesentliche Einblicke in die Lebensgestaltung zu ermöglichen, wird mit Geldstrafe oder einer Freiheitsstrafe von sechs Monaten bis zu zehn Jahren bestraft. –

c) In Bezug auf § 303a StGB

Möchte man die Strafbarkeitslücken im Hinblick auf den digitalen Hausfriedensbruch mittels einer Schadsoftware schließen, so wäre dies nach Eisele/ Nolte dadurch möglich, dass der Tatbestand des § 303a StGB um die Handlungsvariante des „unbefugten Einschleusens eines Programmcodes in ein Informationssystem“ ergänzt wird.[85]

d) Stellungnahme

Diesem Vorschlag zur Ergänzung des § 303a StGB ist beizupflichten, da es durch diese Erweiterung möglich ist, den digitalen Hausfriedensbruch mittels einer Schadsoftware unzweifelhaft unter Strafe stellen zu können.

V. Fazit

Abschließend ist festzuhalten, dass der digitale Hausfriedensbruch, insbesondere durch die Normen der §§ 202a, 202b StGB und § 303a StGB, bereits als Straftat erfasst ist. Jedoch wäre es unter Achtung des „Ultima-Ratio-Prinzips“ durch gezielte Gesetzesänderungen möglich, den strafrechtlichen Schutz bezüglich eines digitalen Hausfriedensbruchs zu erweitern und noch eindeutiger zu normieren.
Wirksamer für die Praxis wäre es jedoch, künftig mehr in die Entwicklung von Hard- und Software zu investieren, um eine unbefugte Zugangsverschaffung bestmöglich im Vorhinein verhindern zu können.

80 *Graf,* NStZ 2007, 129 (129).
81 *Eisele/Nolte,* CR 2020, 488 (491).
82 *Eisele*, 4. Kapitel § 6 Rn. 19.
83 *Eisele/Nolte,* CR 2020, 488 (491).
84 *Ernst,* NJW 2007, 2661 (2662); *Eisele/Nolte,* CR 2020, 488 (491).
85 *Eisele/Nolte,* CR 2020, 488 (491).

Zudem sollte in Zukunft noch mehr die Lösung des Problems hinsichtlich der schweren Fassbarkeit vieler Täter durch die Möglichkeit der Anonymisierung und internationalen Arbeitsteilung, insbesondere für die Strafverfolgungsbehörden, ins Auge gefasst werden, denn das Vorhandensein von Rechtsvorschiften ist nur so lange von Bedeutung, wie diese auch durchgesetzt werden können.