Pferde, Würmer, Roboter, Zombies und das Strafrecht? Vom Sinn und Unsinn neuer Gesetze gegen den sog. digitalen Hausfriedensbruch

von Dr. Markus Mavany[*]

Abstract
Der Beitrag nimmt den Gesetzesantrag des Landes Hessen[1] *über die Kodifizierung des sogenannten "Digitalen Hausfriedensbruchs" zum Anlass, sich mit der Notwendigkeit eines solchen Tatbestands zu befassen. Hierbei werden die technischen Grundlagen von Botnetzen dargestellt und die geltende Rechtslage sowie internationale Vorgaben betrachtet. Zudem wird die Frage erörtert, welchem Schutzgut der neu zu schaffende Straftatbestand dienen müsste. Der Autor gelangt zu dem Schluss, dass ein hinreichender Schutz bereits gewährleistet und eine Neukodifizierung abzulehnen ist.*

Because of the Bill of Hessen "for the draft of a criminal amending law – culpability of the unauthorized use of informational systems, the so called unlawful entry in computer systems" – this essay analyzes the need for such New Elements of crime. Therefore the technical basis of botnets is depicted as well as the legal status and international guidelines are being illustrated. Besides the author is discussing the subject of protection of these new elements. As a result, the author postulates that the enacting should be refused.

I. Einleitung

Stellen Sie sich vor, in ihrem Zuhause versteckt sich ein Fremder. Und das monate-, vielleicht jahrelang. Der Fremde könnte ihr Telefon benutzt, Informationen über Sie gesammelt oder Post in Ihrem Namen versandt haben. Zugegeben, die Wahrscheinlichkeit, dass Sie heute Abend so einen Fremden finden, ist gering. Das gilt solange wir uns in der realen Welt aufhalten. Blicken wir in die digitale Welt, stehen die Chancen ungleich besser, einen ungewollten Eindringling zu finden. In vielen Fällen wird es sich bei diesem Eindringling um sogenannte Botware handeln. Diese gliedert das infizierte System in ein Netzwerk ein, mittels dessen eine Vielzahl unterschiedlicher Computerstraftaten begangen werden kann. Sowohl Stimmen aus dem Bundesamt für die Sicherheit in der Informationstechnik (BSI)[2] als auch aus dem BKA[3] beschreiben Botnetze daher als besondere Bedrohung auf dem Gebiet des Cybercrimes. So verwundert es kaum, dass der Ruf nach strafrechtlichen Konsequenzen immer lauter wird. Dieser Ruf scheint in Wiesbaden erhört worden zu sein. Das hessische Justizministerium kündigte Mitte März eine Gesetzesinitiative im Bundesrat an, die mittels Verschärfungen des Strafrechts den Gefahren von Botnetzen begegnen soll.[4] Im Fokus soll dabei nicht die Begehung von Cyberdelikten mithilfe eines Botnetzes stehen, sondern bereits die Infiltration mit der Botware. Damit wäre der Straftatbestand des digitalen Hausfriedensbruchs geschaffen.

Die Berechtigung eines solchen Delikts erscheint offensichtlich. Der Fremde aus dem Ausgangsbeispiel wäre in der realen Welt gem. § 123 I StGB strafbar, wenn er gegen oder ohne den Willen des Hausrechtsinhabers in dessen Wohnung eindringt. Übertragen in die digitale Welt muss das Eindringen in ein System gegen oder ohne den Willen des Berechtigten für sich genommen ebenso zur Strafbarkeit führen.

Auch scheint die Bundesrepublik zur Schaffung des Straftatbestands des digitalen Hausfriedensbruchs verpflichtet zu sein. Beispielsweise durch die Richtlinie über Angriffe auf Informationssysteme[5]. Dort heißt es in Art. 3, dass jeder Mitgliedstaat die erforderlichen Maßnahmen zu treffen hat, um sicherzustellen, dass der vorsätzliche und unbefugte Zugang zu einem Informationssystem als Ganzes oder zum Teil zumindest dann unter Strafe gestellt wird, wenn kein leichter Fall vorliegt. Diese Verpflichtung besteht insoweit, als dass der Zugang durch eine Verletzung von Sicherheitsmaßnahmen erfolgt. Ähnlich formuliert ist Art. 2 des Übereinkommens über Computerkriminalität[6] des Europarates (sog. „Cybercrimekonvention"). Hier-

---

* Akademischer Rat a.Z. Dr. *Markus Mavany* ist wissenschaftlicher Mitarbeiter und Habilitand am Lehrstuhl von Professor Dr. *Mark A. Zöller* an der Universität Trier. Bei dem Beitrag handelt es sich um den um Fußnoten erweiterten Zusammenschnitt zweier Vorträge, die der Verfasser im Rahmen der Veranstaltung „Einblicke" am 27.4.2016 beim Bundeskriminalamt und der Veranstaltung „Rechtliche Grundlagen und gesetzliche Neuerungen im Bereich Cybercrime" am 4.5.2016 an der Deutschen Hochschule für Polizei gehalten hat. Der Vortragsstil wurde beibehalten.

1 BT Drs. 338/16.

2 Bundesamt für die Sicherheit in der Informationstechnik, Die Lage der IT-Sicherheit in Deutschland 2015, S. 30.

3 Bundeskriminalamt, Cybercrime Bundeslagebild 2014, S. 9.

4 S. hierzu die Nachricht „Gesetzesinitiative gegen ‚digitalen Hausfriedensbruch'", abrufbar unter http://www.heise.de/security/meldung/Gesetzesinitiative-gegen-digitalen-Hausfriedensbruch-3133449.html (zuletzt abgerufen am 20.04.2016).

5 Richtlinie 2013/40/EU des Europäischen Parlaments und des Rates vom 12.8.2013 über Angriffe auf Informationssysteme und zur Ersetzung des Rahmenbeschlusses 2005/222/JI des Rates, ABl. EU L 218, S. 8 ff.

6 Übereinkommen über Computerkriminalität vom 23.11. 2001, ETS Nr. 185.

nach muss jede Vertragspartei die erforderlichen Maßnahmen treffen, um den unbefugten Zugang zu einem Computersystem als Ganzem oder zum Teil als Straftat zu umschreiben. Dabei können die Vertragsparteien als Voraussetzung vorsehen, dass die Straftat unter Verletzung von Sicherheitsmaßnahmen, in der Absicht, Computerdaten zu erlangen, in anderer unredlicher Absicht oder unter Verwendung eines verbundenen Computersystems begangen wurde. In beiden Vorschriften ist also die Verpflichtung enthalten, den unbefugten Zugang zu einem Informationssystem – den digitalen Hausfriedensbruch – unter Strafe zu stellen. Es besteht also Handlungsbedarf!?

Ganz so einfach ist die Sache nicht. Denn zum einen existiert bereits ein umfassendes Strafrechtsregime, welches beim Eindringen in ein fremdes System eingreift (dazu unter III.). Insoweit stellt sich die Frage nach der Berechtigung einer weiteren Strafnorm. Zum anderen dient das Strafrecht dem Schutz von Rechtsgütern. Welches Rechtsgut mit einer Strafnorm gegen den digitalen Hausfriedensbruch geschützt werden soll, ist jedoch noch nicht einmal diskutiert worden. Dies mögen einige der Gründe sein, warum der Gesetzgeber bei der Einführung des § 202a StGB das reine Eindringen in ein Computersystem bewusst nicht unter Strafe stellen wollte[7] – und es bisher *so* auch nicht getan hat.

II. Botnetze – technische Grundlagen

Bevor ich mich den skizzierten Problemen zuwende, sollen zumindest die rudimentären technischen Grundlagen dessen, was als digitaler Hausfriedensbruch und als Botnetz bezeichnet wird, erläutert werden.

Der Begriff des Botnetzes steht für einen Verbund vernetzter Systeme, den sogenannten Bots. Die Bots werden mit einer Software (der Botware) infiziert und von einer oder mehreren zentralen Einheiten ferngesteuert, bei denen es sich nicht selten um sog. Command and Control–Server (C&C) handelt. Weil die Bots die Befehle des C&C blind ausführen, werden sie auch Zombie oder Zombiebots genannt. Die Person, die ein solches Botnetz kontrolliert, wird als Botmaster oder Bot-Herder bezeichnet. Als Bot kann dabei jedes mit dem Internet verbundene System in Frage kommen. Dies umfasst neben PCs, Tablets und Smartphones auch Router und Unterhaltungselektronik wie internetfähige Fernseher oder Radios. Selbst Haushaltsgeräte können betroffen sein. So ist mindestens ein Fall bekannt, bei dem ein Kühlschrank Teil eines Botnetzes war.[8]

Die Anwendungsmöglichkeiten von Botnetzen sind vielfältig. Sie können mit der gebündelten Rechenleistung DDos-Attacken durchführen, mittels Keyloggern Tastatureingaben protokollieren oder den Datenbestand und -verkehr der Bots einsehen.[9] Botnetze dienen somit als infrastrukturelle Grundlage der Cyberkriminalität.[10]

Das Bedrohungspotenzial von Botnetzen ist dementsprechend hoch. Die Jahresstatistik für 2015 des Verbands der Internetwirtschaft e.V. weist von über 175.000 der durch das Anti-Botnet-Beratungszentrum gescannten Systeme 38% Infektionen aus.[11] Es wurden über 715.000 infizierte Dateien gefunden.[12] Nach Informationen des BSI wurden in der ersten Jahreshälfte 2015 täglich circa 60.000 Infektionen deutscher Systeme verzeichnet.[13] Hochgerechnet auf das Gesamtjahr ergibt das eine Zahl von 219 Millionen Infektionen in Deutschland. Zudem geht das BSI davon aus, dass täglich mehrere hundert C&C-Server aktiv sind, die jeweils einzeln oder im Verbund ein Botnetz steuern.[14]

Die Zahlen sind mit Vorsicht zu genießen, da zum einen die Dunkelziffer nicht entdeckter Infektionen kaum valide abschätzbar ist. Zum anderen unterliegt die Zahl der Infektionen einer hohen Fluktuation. So sind Systeme, die eine veraltete Software verwenden, besonders gefährdet.[15] Und deren Zahl verändert sich aufgrund von Softwarewechseln und Stilllegungen permanent. Zumindest aber die Größenordnung, wonach 40 % aller internetfähigen Systeme infiziert sein könnten, dürfte die Realität widerspiegeln.[16]

Eingerichtet wird ein Botnetz, grob vereinfacht, indem ein System mit der Botware infiziert wird, man spricht vom Spreading. Dies kann auf unterschiedlichen Wegen geschehen.[17] Relativ selten ist die Methode, einen Rechner direkt durch Aufspielen der Software bspw. mittels eines USB-Sticks oder einer CD-ROM zu infizieren. Wesentlich gebräuchlicher ist die Variante, die Software im Anhang einer E-Mail oder als Teil einer Nachricht in einem Sozialen Netzwerk zu versenden. Der Versand kann durch bereits zuvor gekaperte Bots geschehen. Das heißt die

---

7 Vgl. BT-Drs. 10/5058, S. 258.

8 S. hierzu die Nachricht „Botnetz infiziert Kühlschrank“, abrufbar unter http://www.golem.de/news/thingbot-botnetz-infiziert-kuehlschrank-1401-103978.html (zuletzt abgerufen am 20.04.2016); hierzu auch *Roos/Schumacher*, MMR 2014, 377 (377).

9 Vgl. Bundeskriminalamt, Cybercrime Bundeslagebild 2014, S. 9; Bundesamt für die Sicherheit in der Informationstechnik, Die Lage der IT-Sicherheit in Deutschland 2015, S. 30.

10 Zum gleichen Schluss gelangen auch das Bundesamt für die Sicherheit in der Informationstechnik (Die Lage der IT-Sicherheit in Deutschland 2015, S. 30) und der Branchenverband der Internetwirtschaft, vgl. die Ausführungen auf der vom Branchenverband zur Verfügung gestellten Plattform botfrei.de, abrufbar im Internet unter https://www.botfrei.de/informieren.html (zuletzt abgerufen am 20.04.2016). Ein plakatives Beispiel liefert die Entscheidung des *LG Düsseldorf*, Urt. v. 22.3.2011 – 3 KLs 1/11 (=MMR 2011, 624 f.).

11 Jahresstatistik 2015 des Verbandes der Internetwirtschaft e.V., abrufbar im Internet unter https://www.eco.de/2016/pressemeldungen/botfrei-de-jahresstatistik-2015-zahl-der-zombierechner-weiter-bedrohlich.html (zuletzt abgerufen am 20.4.2016).

12 A.a.O.

13 Bundesamt für die Sicherheit in der Informationstechnik, Die Lage der IT-Sicherheit in Deutschland 2015, S. 30.

14 A.a.O., S. 30.

15 Jahresstatistik 2015 des Verbandes der Internetwirtschaft e.V., abrufbar im Internet unter https://www.eco.de/2016/pressemeldungen/botfrei-de-jahresstatistik-2015-zahl-der-zombierechner-weiter-bedrohlich.html (zuletzt abgerufen am 20.4.2016).

16 A.a.O.; mit Bezug hierzu auch Bundeskriminalamt, Cybercrime Bundeslagebild 2014, S. 9.

17 Ausführlich zu den technischen Wegen des Spreading *Wagner*, IT-Security und Botnetze, Aktuelle Angriffs- und Abwehrmethoden, 2011, S. 27 – 28.

Botware übernimmt ein System, loggt sich in den vorhandenen E-Mail Client oder Facebook-Account ein und versendet sich selbst an alle gespeicherten Kontakte. Zum Teil wird die Software als Trojaner in anderen Programmen oder Dateien versteckt. Stark zugenommen hat die Infizierung mit der Methode des Drive-by-infection[18]. Die Botware wird bei dieser Methode auf einem infizierten Server versteckt. Wenn dort gespeicherte Websites aufgerufen werden, wird automatisch auch die Botware im Hintergrund geladen. All diesen Infizierungsmöglichkeiten ist gemeinsam, dass sie dem jeweiligen Nutzer des Geräts im Regelfall verborgen bleiben.
Einmal eingedrungen stellt die Botware eine Verbindung zum C&C her und meldet Bereitschaft. In diesem Moment wird das Gerät zum Bot. Der Botmaster kann nun Befehle an den Bot senden.

Betrachtet man die technischen Grundlagen, so kann man drei Phasen in Bezug auf den Aufbau und Betrieb von Botnetzen identifizieren. Die Erste Phase besteht in dem Programmieren der für die Fernsteuerung der Bots notwendigen Software. Die zweite Phase umfasst das Spreading, also die Infizierung der Geräte mit der Botware. In der dritten Phase wird das Botnetz dann zu weiteren Aktionen verwendet.
Sobald die Botware auf das System installiert ist, wird von einem digitalen Hausfriedensbruch gesprochen. Eine Verbindung zum C&C oder die Ausführung von Befehlen ist nicht notwendig. Bereits die reine Infiltration, also das „Betreten" des Systems, ist ausreichend. Der digitale Hausfriedensbruch im Zusammenhang mit Botnetzen wird somit in deren zweiter Phase, dem Spreading, verwirklicht.

III. Strafrechtliche Behandlung von Botnetzen

Unterzieht man diese zweite Phase einer strafrechtlichen Bewertung, so können sich diverse Strafbarkeiten ergeben. Insbesondere kommen die Tatbestände der §§ 202a, 202b und 303a StGB und § 44 Abs. 1 i.V.m. § 43 Abs. 2 Nr. 1, 4 BDSG in Betracht.

Mit dem § 202a StGB hat der Gesetzgeber das Ausspähen von Daten unter Strafe gestellt. Der Tatbestand wurde bereits 1986 in das StGB eingefügt[19] und zuletzt durch das 41. StrÄndG[20] aus dem Jahr 2007 reformiert. Diese Änderung diente auch der Umsetzung der Cybercrimekonvention des Europarates und des Art. 2 des Rahmenbeschlusses[21] über Angriffe auf Informationssysteme.[22] Der Rahmenbeschluss wurde zwischenzeitlich durch die erwähnte Richtlinie über Angriffe auf Informationssysteme ersetzt. Deren Art. 3 entspricht nahezu wortgleich dem mit dem 41. StrÄndG umgesetzten Art. 2 des Rahmenbeschlusses. Die Reform zielte vor allem darauf, das bis zum Jahr 2007 straflose sog. Hacking, also das computertechnische Überwinden von Zugangssperren zur Verschaffung der Zugangsmöglichkeiten auf Daten in die Strafbarkeit des § 202a StGB einzubeziehen.[23]

Nach § 202a Abs. 1 StGB macht sich strafbar, wer sich oder einem anderen unbefugt Zugang zu Daten, die nicht für ihn bestimmt und gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung dieser Zugangssicherung verschafft. Hierbei ist in Bezug auf den digitalen Hausfriedensbruch zweierlei zu beachten:
Erstens schützt § 202a StGB eine formale Geheimnissphäre. Geschützt ist die Verfügungsbefugnis des Berechtigten an dem gedanklichen Inhalt der Daten, aber nur soweit der Dateninhaber durch eine Zugangssicherung ein besonderes Geheimhaltungsbedürfnis dokumentiert hat.[24] Die Zugangssicherung muss durch den Täter überwunden werden. Dabei sind die Anforderungen an die Zugangssicherung gering. Sie muss nur objektiv geeignet sein und subjektiv dazu dienen, den Zugriff Dritter auf die Daten zu verhindern.[25] Ob dies effektiv geschieht und ihr einziger Zweck ist, ist unerheblich. Somit reicht bereits die Vergabe eines Passwortes oder die Verschlüsselung von Daten aus.[26] Besteht eine solche Sicherungsmaßnahme nicht, ist § 202a StGB nicht erfüllt. Dies gilt auch, wenn das System mit einer Malware infiziert, also computertechnisch „Betreten" wird.
Zweitens ist gefordert, dass sich der Täter Zugang zu den tatbestandlichen Daten verschafft. Bei dem Begriff des „Zugangs" könnte man auf die Idee kommen, dass ein solcher vorliegt, wenn man ein System infiltriert, sich quasi digitalen Zugang zum System verschafft. Ein i.S.d. § 202a StGB tatbestandlicher Zugang liegt jedoch dann vor, wenn der Täter in der Lage ist, die Daten sichtbar zu machen.[27] Er muss die Daten nicht tatsächlich eingesehen haben. Es reicht aus, wenn er auf die Daten zugreifen könnte, wenn er wollte.[28] Der Zugang kann somit computertechnisch, z.B. durch das Einschleusen einer Malware auf das System vermittelt werden, wie es bei der Errichtung von Botnetzen üblich ist. Es ist jedoch auch möglich, einen USB-Stick aus einem Tresor zu stehlen und sich auf diese Weise den Zugang zu den auf dem Stick gespeicherten und durch den Tresor gesicherten Daten zu verschaffen.[29] Ein computertechnisches Eindringen in das System ist somit für die Verwirklichung des § 202a StGB nicht erforderlich.

---

18 S. zum Begriff die Erläuterungen in Bundeskriminalamt, Cybercrime Bundeslagebild 2014, S. 7 mit Fn. 11; *Roos/Schumacher*, MMR 2014, 377 (378 mit Fn. 8).

19 2. Gesetz zur Bekämpfung der Wirtschaftskriminalität vom 15.5.1986, BGBl. I 1986, S. 721 – 729; s. hierzu auch BT-Drs. 10/5058, S. 28.

20 41. Strafrechtsänderungsgesetz zur Bekämpfung der Computerkriminalität vom 7. 8. 2007, BGBl. I 2007, S. 1786 f.

21 Rahmenbeschluss 2005/222/JI des Rates vom 24.2.2005 über Angriffe auf Informationssysteme, Abl. EU L 69, S. 67.

22 Vgl. BT-Drs. 16/5449, S. 1; *Schumann*, NStZ 2007, 675 (675); *Ernst*, NJW 2007, 2661 (2661).

23 *Popp*, in: AnwK-StGB, 2. Aufl. (2015), § 202a Rn. 1; *Ernst*, NJW 2007, 2661 (2661); *Schumann*, NStZ 2007, 675 (675 f.).

24 *Graf*, in: MüKo-StGB, Bd. 4, 2. Aufl. (2012), § 202a Rn. 2; *Lenckner/Eisele*, in: Schönke/Schröder, 29. Aufl. (2014), § 202a Rn. 1; *Eisele*, Computer- und Medienstrafrecht, 2013, § 6 Rn. 1; krit. *Dietrich*, NStZ 2011, 247 ff.

25 *Eisele*, in: Schönke/Schröder, § 6 Rn. 15; *Popp*, in: AnwK-StGB, § 202a Rn. 7 – 9; *Graf*, in MüKo-StGB, § 202a Rn. 35 m. Bsp.

26 *Roos/Schumacher*, MMR 2014, 377 (379); *Lenckner/Eisele*, in: Schönke/Schröder, § 202a Rn. 15.

27 *Lenckner/Eisele*, in: Schönke/Schröder, § 202a Rn. 18; *Popp*, in: AnwK-StGB, § 202a Rn. 10; BT-Drs. 16/3656, S. 9.

28 *Lenckner/Eisele*, in: Schönke/Schröder, § 202a Rn. 18; *Popp*, in: AnwK-StGB, § 202a Rn. 10; BT-Drs. 16/3656, S.9.

29 *Popp*, in: AnwK-StGB, § 202a Rn. 7.

Ein digitaler Hausfriedensbruch kann somit von § 202a StGB erfasst sein, zwingend ist dies nicht. Daher wird es jeweils Tatfrage sein, ob bereits durch das Eindringen der Botware in das vernetzte System eine Strafbarkeit nach dieser Norm besteht. Doch eine Botware, die nicht auch in der Lage ist, sich Zugang zu gesicherten Daten zu verschaffen, wird dem kriminellen Botmaster kaum weiterhelfen. Denn das Botnetz soll ja gerade der Begehung weiterer Straftaten dienen, wozu die Daten der Betroffenen erforderlich sind. Daher wird die Botware über die Eingliederung des infizierten Systems in das Netzwerk zusätzlich die Funktionen bieten, fremde Daten in Form des § 202a StGB auszuspähen. So beispielsweise durch keylogging, passwordsniffing oder ähnliches. Und heutzutage verfügt praktisch jedes System über die erforderlichen Sicherungsmaßnahmen, sei es durch eine Tastensperre, eine Firewall oder ein Log-in.
Festzuhalten bleibt, dass § 202a StGB nicht die computertechnische Infiltration eines vernetzten Systems und damit den digitalen Hausfriedensbruch erfordert. Im Ergebnis wird § 202a Abs. 1 StGB in der Phase des Spreadings dennoch bis auf seltene Ausnahmen verwirklicht.[30] Daher wird der § 202a StGB bereits jetzt als Straftatbestand zur Erfassung des digitalen bzw. elektronischen Hausfriedensbruchs bezeichnet.[31]

Zum vergleichbaren Ergebnis gelangt man, wenn man eine mögliche Strafbarkeit gem. § 44 Abs. 1 i.V.m. § 43 Abs. 2 Nr. 1, 4 BDSG in den Blick nimmt. Nach § 43 Abs. 2 Nr. 1 BDSG handelt derjenige ordnungswidrig, der vorsätzlich oder fahrlässig unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, erhebt oder verarbeitet. § 43 Abs. 2 Nr. 4 BDSG normiert eine Ordnungswidrigkeit in den Fällen, in denen jemand vorsätzlich oder fahrlässig die Übermittlung von personenbezogenen Daten, die nicht allgemein zugänglich sind, durch unrichtige Angaben erschleicht. Auch durch diese Regelungen sollten Hacker-Angriffe erfasst werden.[32] Ob die Infektion eines Systems mit einer Botware von § 43 Abs. 2 Nr. 1, 4 BDSG umfasst wird, ist ebenso wie bei § 202a StGB Tatfrage und danach zu beantworten, ob die Botware personenbezogene Daten erhebt, verarbeitet oder übermittelt. Unter der Verarbeitung ist gem. § 3 Abs. 4 BDSG das Speichern, Verändern, Übermitteln, Sperren oder Löschen personenbezogener Daten zu verstehen. Technisch notwendig ist eine solche Verarbeitung für eine Botware nicht. Doch wie schon bei § 202a StGB wird die Botware dies praktisch immer auch leisten. Denn die Erlangung personenbezogener Daten ist Voraussetzung für die Verwirklichung weiterer Cybercrimedelikte wie z.B. eines Computerbetrugs gem. § 263a StGB mittels ausgespähter Zugangsberechtigungen.

Zur Straftat wird dieses Verhalten gem. § 44 Abs. 1 BDSG wenn der Täter gegen Entgelt oder in der Absicht handelt, sich oder einen anderen zu bereichern oder einen anderen zu schädigen. Oftmals werden Botnetze installiert, damit der Botmaster das Netzwerk anderen Kriminellen zur Verfügung stellen kann. Er ist praktisch ein Dienstleister im Bereich der Cyberkriminalität. Hieraus kann die notwendige Bereicherungsabsicht ebenso folgen, wie aus dem Plan des Botmasters, das Botnetz selbst zu kriminellen Zwecken einzusetzen. Die Schädigung Dritter ist dann ein notwendiges Zwischenziel und daher auch zu bejahen.

Ebenfalls im Bereich des Möglichen liegt eine Strafbarkeit gem. § 202b StGB durch die Infektion. Nach § 202b StGB macht sich strafbar, wer sich mittels technischer Anlagen unbefugt Daten verschafft, die sich im elektronischen Übertragungsvorgang befinden. Hierdurch werden die Inhalte aller elektronischer Datenübermittlungsvorgänge erfasst, sei es E-Mail, Telefon, Voice over IP, Fax, WLAN-Übertragung, Bluetooth, etc.[33] § 202b StGB kann erfüllt sein, wenn die Infektion durch Zugriff auf eine Datenübertragung erfolgt, beispielsweise wenn durch einen infizierten E-Mailserver alle ein- und ausgehenden E-Mails abgefangen und mit dem schadhaften Anhang weitergeleitet werden.[34]

Zudem kann durch die Infektion eine Strafbarkeit gem. § 303a StGB in Betracht kommen. In der Norm ist die Datenveränderung strafrechtlich erfasst. Es wird jedes rechtswidrige Löschen, Unterdrücken, Unbrauchbarmachen oder Verändern von Daten unter Strafe gestellt.
§ 303a StGB schützt die Integrität und Verwendbarkeit eines gespeicherten Datenbestandes.[35] Nur der Berechtigte kann straflos Änderungen herbeiführen. Nicht geschützt ist die Integrität eines Speichermediums an sich. Das heißt, dass ein tatbestandliches Verändern des Datenbestandes nur vorliegt, wenn die bereits auf einem Speichermedium vorhandenen Daten inhaltlich umgestaltet werden.[36] Wer ohne einen solchen inhaltlichen Eingriff lediglich Daten hinzufügt, erfüllt den Tatbestand nicht. Dies bedeutet, dass das bloße Eindringen in das und die Installation der Botware auf das System zunächst keine Datenveränderung i.S.d. § 303a StGB darstellen. Greift die Botware im Zuge der Installation jedoch auf vorhandene Daten zu und führt dort zu inhaltlichen Veränderungen, ist § 303a StGB erfüllt. In Anbetracht des Umstandes, dass die Botware für ihr Funktionieren die Zuweisungen von Ressourcen des Systems verändern und bestehende Protokolle umschreiben muss, ist auch dieser Tatbestand gegeben.

---

30 Ebenso *Lenckner/Eisele*, in: Schönke/Schröder, § 202a Rn. 18; *Roos/Schumacher*, MMR 2014, 377 (379); beachte aber *Gröseling/Höfinger*, MMR 2007, 549 (551) und *Gercke*, ZUM 2007, 283 (283), die jeweils auf denkbare Abweichungen hinweisen.

31 So etwa *Gröseling/Höfinger*, MMR 2007, 549 (551); *Ernst*, NJW 2007, 2661 (2661); *Sieber*, in: Hoeren/Sieber/Holznagel (Hrsg), Handbuch Multimedia-Recht, Loseblatt, 45. EL, Stand: 6/2015, Teil 19 Rn. 418.

32 Vgl. BT-Drs. 11/4306, S. 55 zur alten Rechtslage; ebenso *Gola/Schumerus*, BDSG, 12. Aufl. (2015), § 43 Rn. 23; *Roos/Schumacher*, MMR 2014, 377 (379).

33 *Eisele*, in: Schönke/Schröder, § 202b Rn. 4; *Popp*, in: AnwK-StGB, § 202b Rn. 3; *Graf*, in: MüKo-StGB, § 202b Rn. 9; *Ernst*, NJW 2007, 2661 (2662).

34 *Graf*, in: MüKo-StGB, § 202b Rn. 16; *Eisele*, Computer- und Medienstrafrecht, 2013, § 7 Rn. 39.

35 *Popp*, in: AnwK-StGB, § 303a Rn. 1; *Hilgendorf/Frank/Valerius*, Computer- und Internetstrafrecht, 2. Aufl. (2012), Rn. 192; *Eisele*, § 9 Rn. 62.

36 *Ernst*, NJW 2003, 3233 (3238); *Popp*, in: AnwK-StGB, § 303a Rn. 10; *Eisele*, § 9 Rn. 76.

Neben der skizzierten Strafbarkeit könnte bei einer erheblichen Beeinträchtigung von IT-Anlagen durch die Installation der Botware auch eine Computersabotage gem. § 303b StGB verwirklicht werden. Eine solche Beeinträchtigung realisiert sich zumeist erst in der dritten Phase, der Nutzung des Botnetzes zu kriminellen Zwecken. Letztlich kommen auch die Straftatbestände des TKG im Falle des Abhörens von Individualkommunikation in Betracht. Sofern sich die Fälle nicht schon mit denen der §§ 202a, 202b StGB decken, werden auch diese Tatbestände weitgehend erst in der dritten, hier nicht zu betrachtenden Phase verwirklicht werden.

Es bleibt somit festzuhalten, dass in der Phase des Spreadings durch die Infektion mit einer Botware die Tatbestände der §§ 202a und 303a StGB, 44 Abs. 1 i.V.m. 43 Abs. 2 Nr. 1, 4 BDSG erfüllt werden. Zudem kann auch eine Strafbarkeit gem. § 202b StGB gegeben sein.

IV. Sinn und Unsinn eines Straftatbestandes gegen den Digitalen Hausfriedensbruch

Aus dem Gesagten können wir ersehen, dass eine weitreichende Strafbarkeit in der Spreadingphase von Botnetzen bereits besteht. De lege lata nicht kriminalisiert ist hingegen der – wohl theoretische – Fall, in dem der Täter zwar in das fremde System eindringt, indem er dort eine Botware installiert, diese jedoch weder in der Lage ist, gesicherte oder personenbezogene Daten einzusehen, noch in den vorhandenen Datenbestand inhaltlich einzugreifen oder Nutzer- und/oder Nutzungsdaten zu erheben. Dieser Zustand reicht nach zutreffender Ansicht zur Umsetzung der dargestellten inter- und supranationalen Vorgaben von EU und Europarat aus.[37] Damit setzt sich ein möglicher Straftatbestand gegen den digitalen Hausfriedensbruch dem Vorwurf aus, rein symbolisches Strafrecht zu verwirklichen.
Jedoch könnte die Kriminalisierung trotz dieser Bedenken seine Berechtigung haben. Denn es ist durchaus denkbar, dass das bestehende Strafrechtsregime nicht die Beeinträchtigung aller tangierten Rechtsgüter abbildet. Insbesondere nicht das Schutzgut des digitalen Hausfriedenbruchs erfasst. Es gilt daher zu beantworten, was überhaupt das Schutzgut eines neu zu schaffenden Tatbestands des digitalen Hausfriedenbruchs wäre.
Der Blick führt hierbei zunächst auf das analoge Vorbild, den § 123 StGB. Dessen Schutzgut ist umstritten. Die h.M.[38] sieht zu Recht das Hausrecht als geschützt an. Dieses Recht beinhaltet die Freiheit zu bestimmen, wer sich innerhalb einer bestimmten räumlichen Sphäre aufhalten darf und wer nicht.[39] Übertragen auf den digitalen Hausfriedenbruch müsste somit ein digitales Hausrecht bestehen, vermöge dessen der Inhaber darüber bestimmen kann, wer sich in einer bestimmten digitalen Sphäre aufhalten darf und wer nicht. Dies birgt kaum absehbare Bestimmtheitsprobleme. Bereits die Definition der digitalen Sphäre lässt sich nicht bestimmt erreichen. Soll es sich hierbei um die in einem Computersystem verfügbaren Speicherkapazitäten handeln, also um Festplatte, RAM, Cache usw.? Und falls ja, erfasst dies auch mobile Speichermedien wie SD-Karten und USB-Sticks? Gilt das nur, wenn diese mit dem Hauptsystem verbunden oder auch dann, wenn sie hiervon entfernt worden sind? Und was passiert, wenn das Medium mit einem anderen System verbunden wird? Wird es dann Teil des neuen Systems oder ist es dem Alten zuzuordnen?
Selbst wenn sich eine klare Umgrenzung der digitalen Sphäre erreichen ließe, etwa anhand der Zuordnung zur Hardware, ergeben sich mit Blick auf die technische Realität weitere Probleme. So sind die digitalen Sphären, in denen sich eine Person bewegt, in Zeiten von flächendeckender mobiler Vernetzung und Cloud Computing mehr als diffus. Wenn die Daten, auf die ein Nutzer zugreifen möchte, und die Programme, denen er sich hierzu bedient, gar nicht mehr auf der eigenen Hardware gespeichert sind, so verkümmert die digitale Sphäre bei dem skizzierten hardwareorientierten Verständnis zu einer bloßen Tür ohne geschützten Raum.
Auch fragt sich, wer eigentlich der Inhaber des digitalen Hausrechts sein soll. Wäre dies wiederum hardwarebezogen zu interpretieren, läge der Schluss nahe, dem Eigentümer des Systems das digitale Hausrecht zuzusprechen. Doch die Eigentumsverhältnisse lassen kaum einen Rückschluss auf die Person zu, die durch den digitalen Hausfriedensbruch tangiert wird. So beispielsweise wenn ein Computer von mehreren Familienmitgliedern genutzt wird. Zwar ist anerkannt, dass im Rahmen des § 123 StGB das reale Hausrecht mehreren Personen zustehen kann.[40] Bei dem gemeinsam genutzten Familien-PC mag das auch in Bezug auf eine digitale Sphäre nachvollziehbar sein. Anders bei geleasten Systemen, man denke an Firmenserver oder Firmenlaptops. Hier weichen Nutzer, Eigentümer und Dateninhaber voneinander ab. Zudem werden oft private und dienstliche Datenbestände miteinander vermischt. Gleiches gilt bei finanzierten Systemen, die unter Eigentumsvorbehalt stehen. Hiervon sind viele Smartphones betroffen, die im Rahmen eines Mobilfunkvertrags finanziert werden. Ein ähnliches Problem stellt sich mit Blick auf vermietete oder verliehene Geräte wie WLAN-Router, die vom Accessprovider für die Dauer eines Vertrages überlassen werden.

Will man das digitale Hausrecht dagegen dem Nutzer des Systems zubilligen, so stellt sich die Frage, ob es nur insoweit besteht, wie der Nutzer tatsächlich über das System verfügen kann, oder ob es sich auf das Gesamtsystem erstreckt. Wieso aber im letzten Fall ein Nutzer in seinem digitalen Hausrecht beeinträchtigt sein soll, wenn die Botware nur in diesem Nutzer nicht zur Verfügung stehende Ressourcen oder Datenbestände eingreifen kann, erschließt sich nicht.

---

37 So z.B. *Ernst*, NJW 2007, 2661 (2661); *Schumann*, NStZ 2007, 675 (675 f.)

38 *Lenckner/Sternberg-Lieben*, in: Schönke/Schröder, § 123 Rn. 1; *Fischer*, StGB, 63. Aufl. (2016), § 123 Rn. 2; *Ostendorf*, in: NK, 4. Aufl. (2013), § 123 Rn. 3; *Schäfer*, in: MüKo-StGB, Bd. 3, 2. Aufl. (2012), § 123 Rn. 1; *Lilie*, in: LK-StGB, Bd. 5, 12. Aufl. (2009), § 123 Rn. 159.

39 *Schäfer*, in: MüKo-StGB, § 123 Rn. 2; *Graf v. Schlieffen*, in: AnwK-StGB, § 123 Rn. 1; *Lilie*, in: LK-StGB, § 123 Rn. 1; *Sternberg-Lieben*, in: Schönke/Schröder, § 123 Rn. 1; s. auch *OLG Frankfurt,* NJW 2006, 1746 (1749).

40 BGHSt 21, 224 (226); *Sternberg-Lieben*, in: Schönke/Schröder, § 123 Rn. 18; *Fischer*, § 123 Rn. 4; *Graf v. Schlieffen*, in: AnwK-StGB, § 123 Rn. 11 f.

Ein digitales Hausrecht strafrechtlich zu schützen geht daher schon im Ansatz an der technischen Realität vorbei und sieht sich nicht lösbaren rechtlichen Bestimmtheitsproblemen gegenüber. Ein digitales Hausrecht kommt damit als Schutzgut eines Straftatbestands gegen den digitalen Hausfriedensbruch nicht in Frage.

Berücksichtigt man, dass die Infiltration eines Systems die Nutzung des dort vorhandenen Speicherplatzes und dessen Ressourcen bedingt, so könnte man als Schutzgut des digitalen Hausfriedensbruchs das Eigentum an dem infiltrierten System annehmen. Mit der Nutzung des Systems ist die umfassende Verfügungsgewalt des Eigentümers eingeschränkt, so dass eine Rechtsgutsbeeinträchtigung gegeben wäre. Auch wird diese Eigentumsbeeinträchtigung durch die bestehenden Straftatbestände der §§ 202a, 202b, 303a und 303b StGB nicht erfasst. Jedoch wären auch hier die skizzierten Probleme in Bezug auf ein Abweichen von Eigentümer, Nutzer und Dateninhaber ungelöst. Auch hat der Gesetzgeber aus gutem Grund die reine Nutzungsentziehung nur in dem begrenzten Umfang des § 248b StGB strafrechtlich erfasst.[41] Zudem ist zu berücksichtigen, dass die Botware zumeist nur zuvor ungenutzte Ressourcen verwendet oder im Hinblick auf die Gesamtleistungsfähigkeit des Systems einen äußerst geringen Ressourcenbedarf aufweist. Belegen lässt sich dieser Umstand daran, dass die meisten Betroffenen erst von der Eingliederung ihrer Systeme in ein Botnetz erfahren, wenn sie von den Behörden darauf hingewiesen werden.[42] Daher ist die Eigentumsbeeinträchtigung am System durch den digitalen Hausfriedensbruch als so gering anzusehen, dass die strafrechtliche Erheblichkeitsschwelle nicht überschritten wird. Besonders eindringlich wird dies an dem Beispiel des eingangs genannten Kühlschrank-Bots deutlich. Dessen Eigentümer kann ohne Frage sein kaltes Bier genießen, gleichgültig ob der Kühlschrank in ein Botnetz eingegliedert ist oder nicht. Auch das Eigentum scheidet somit als potenzielles Schutzgut des digitalen Hausfriedenbruchs aus.

Man könnte mit einem Blick in das Verfassungsrecht auf der Suche nach dem Schutzgut fündig werden. Denn der Schutz informationstechnischer Systeme vor unbefugtem Zugriff ist seit der Online-Durchsuchung-Entscheidung des *BVerfG*[43] als grundrechtlich verbürgt anerkannt. Die Verbürgung erfolgt innerhalb des Allgemeinen Persönlichkeitsrechts in der Ausprägung des Rechts auf die Integrität und Vertraulichkeit informationstechnischer Systeme[44], welche auch als Computergrundrecht[45] bezeichnet wird. Geschützt wird in Bezug auf Eingriffe des Staates gegenüber den Bürgern. Mit dem Gedanken der mittelbaren Drittwirkung von Grundrechten[46] und dem Bedürfnis nach einem adäquaten Persönlichkeitsschutz auch gegenüber Privaten lässt sich der Schutzgedanke auf das materielle Strafrecht übertragen. Das *BVerfG* hat in der Entscheidung anerkannt, dass der Einzelne zu seiner Persönlichkeitsentfaltung auf die Nutzung informationstechnischer Systeme angewiesen ist.[47] Dies umfasst neben der Kommunikation und Interaktion mit anderen auch den Konsum von digitalen Medienangeboten wie Filmen und Musik oder die bloße Information über Websites etc. Werden die informationstechnischen Systeme zur Persönlichkeitsentfaltung genutzt, fallen zwangsläufig Unmengen an persönlichkeitsrelevanten Daten an, die der Nutzer entweder selbst in das System eingibt oder die das System bei der Nutzung generiert.[48] Die Fülle dieser Informationen könnte in Umfang und Vielfalt durch einen Eingriff auf das System einen Einblick in wesentliche Teile der Lebensgestaltung einer Person ermöglichen oder gar ein aussagekräftiges Bild der Persönlichkeit des Betroffenen offenbaren.[49] Müsste der Einzelne nun befürchten, dass diese Daten von einer staatlichen Stelle – oder im Falle einer Infektion durch Cyberkriminelle von privaten Dritten – erhoben und verarbeitet werden, stünde zu befürchten, dass er aufgrund dieser Möglichkeit sein Nutzungsverhalten und damit seine Persönlichkeitsentfaltung anpasst.[50] Daher schützt das als Computergrundrecht bezeichnete Recht das Interesse des Nutzers, dass die vom System erzeugten, verarbeiteten oder gespeicherten Daten in der Gesamtheit vertraulich bleiben.[51] Somit darf auf das System nicht zugegriffen werden, weil auf diese Weise die entscheidende Hürde für die Ausspähung, Überwachung oder Manipulation des Systems sowie eine weitere Datenerhebung überschritten ist.[52]

Demnach passt das Computergrundrecht als Schutzgut für den Tatbestand des digitalen Hausfriedensbruchs perfekt.

Wer nun aber glaubt, mit Archimedes „Heureka“ schreien zu können, weil die Lösung des Problems gefunden ist, der wird enttäuscht. Denn auch in Bezug auf dieses Schutzgut sind noch viele Fragen ungeklärt. Insbesondere fragt sich, wie schon beim digitalen Hausrecht, wem das Rechtsgut der Vertraulichkeit und Integrität des informationstechnischen Systems eigentlich zusteht. Diese Frage

41 Der unbefugte Gebrauch fremden Eigentums ist danach nur in Bezug auf Fahrzeuge unter Strafe gestellt. Diese systemfremde Regelung erklärt sich aus der historischen Entwicklung der Norm, die im Wortlaut dem § 1 Abs. 1, 2, 3 und 5 der (Not-)Verordnung des Reichspräsidenten gegen den unbefugten Gebrauch von Kraftfahrzeugen und Fahrrädern vom 20.10.1932 entspricht; *Hohmann*, in: MüKo-StGB, § 248b Rn. 2, 5; im Einzelnen zum Tatbestand s. *Zöller*, Strafrecht BT I, 2. Aufl. (2015), Rn. 110 – 120.

42 Vgl. Bundeskriminalamt, Cybercrime Bundeslagebild 2014, S. 9; Jahresstatistik 2015 des Verbandes der Internetwirtschaft e.V. auf botfrei.de, abrufbar im Internet unter https://www.eco.de/2016/pressemeldungen/botfrei-de-jahresstatistik-2015-zahl-der-zombierechner-weiter-bedrohlich.html (zuletzt abgerufen am 20.04.2016).

43 *BVerfG*, Urt. v. 27.2.2008 – 1 BvR 370/07, 1 BvR 595/07 = NJW 2008, 822 – 837.

44 *BVerfG,* NJW 2008, 822 (824); hierzu *Murswiek*, in: Sachs, GG, 7. Aufl. (2014), Art. 2 Rn. 73c; *Pieroth/Schlink/Kingreen/Poscher*, Grundrechte Staatsrecht II, 31. Aufl. (2015), Rn. 417; *Ipsen*, Staatsrecht II Grundrechte, 18. Aufl. (2015), Rn. 325a f.

45 Vgl. *Murswiek*, in: Sachs, Art. 2 Rn. 73c; *Ipsen*, Rn. 325a f.; *Kutscha*, DuD 2012, 391 (391).

46 Vgl. grundlegend *Ipsen*, Rn. 70; *Pieroth/Schlink/Kingreen/Poscher*, Rn. 203.

47 *BVerfG,* NJW 2008, 822 (824).

48 A.a.O., 824 f.

49 A.a.O., 827.

50 A.a.O., 825.

51 A.a.O., 827.

52 A.a.O., 827); hierzu *Murswiek*, in: Sachs, Art. 2 Rn. 73c f.

kann hier jedoch eindeutig beantwortet werden: Es geht bei dem durch das Computergrundrecht vermittelten Schutz nicht um das Verfügungsrecht über eine wie auch immer geartete Sphäre, sondern um die Sicherung der entscheidenden Hürde, die einem umfassenden Zugriff auf und der Erhebung von Daten entgegensteht. Daher muss derjenige geschützt werden, dessen Daten durch die Infektion des Systems betroffen wären, also der Dateninhaber. Letztlich wäre dessen Interesse an der Geheimhaltung der Daten protektiert. Das Computergrundrecht strafrechtlich über einen Tatbestand des digitalen Hausfriedensbruchs zu schützen bedeutet somit nichts anderes, als einen strafrechtlichen Vorfelddatenschutz zu etablieren. Und hier beißt sich die Katze in den Schwanz. Denn der Dateninhaber und dessen Geheimhaltungsinteressen sind bereits durch die §§ 202a StGB, 43 Abs. 2 Nr. 4 BDSG umfassend geschützt.[53]

V. Fazit

Zusammenfassend ist festzuhalten:

1. Unter dem Begriff des digitalen Hausfriedenbruchs ist das computertechnische Eindringen in ein informationstechnisches System zu verstehen.
2. Der digitale Hausfriedensbruch wird in der Phase des Spreading verwirklicht.
3. De lege lata besteht eine weitreichende Kriminalisierung der Spreadingphase. Je nach Ausgestaltung der Botware ist das Spreading von den §§ 202a, 202b, 303a StGB und § 44 I i.V.m. § 43 II Nr. 4 BDSG erfasst.
4. Will man das Eindringen in ein informationstechnisches System darüber hinaus weiter kriminalisieren, kann dies nur zum Schutz eines Rechtsguts erfolgen, das von den Schutzgütern der verwirklichten Tatbestände abweicht.
5. Der Schutz eines digitalen Hausrechts parallel zum realen Hausrecht i.S.d. § 123 StGB ginge an der technischen Realität vorbei und sieht sich nicht überwindbaren Bestimmtheitsproblemen ausgesetzt.
6. Auch das Eigentum an dem System scheidet als Schutzgut aus.
7. Möglich wäre es, das allgemeine Persönlichkeitsrecht aus Art. 2 I i.V.m. Art. 1 I GG in seiner Ausprägung als Recht auf die Vertraulichkeit und Integrität informationstechnischer Systeme als Schutzgut zu deklarieren.
8. Ein solchermaßen vermittelter Schutz stünde jedoch nur dem Dateninhaber mit Blick auf seine Geheimhaltungsinteressen an den Daten zu. Dieser Schutz ist bereits durch die §§ 202a StGB, 43 Abs. 2 Nr. 4 BDSG strafrechtlich gewährleistet.

Im Ergebnis ist die Schaffung eines neuen Straftatbestands des digitalen Hausfriedenbruchs daher abzulehnen. Weder aus internationalen Vorgaben, noch mit Blick auf das potenzielle Schutzgut ergibt sich die Notwendigkeit einer weiteren Kriminalisierung. Daher gilt auch hier, wie bei vielen gesetzgeberischen Initiativen der letzten Zeit: Wir benötigen keine neuen Strafnormen, sondern mehr Mittel für die Strafverfolgungsbehörden, um die bestehenden Tatbestände effektiv durchzusetzen.

[53] Insoweit zweifelt *Murswiek* auch die Notwendigkeit des Computergrundrechts neben dem Recht auf informationelle Selbstbestimmung an, *Murswiek*, in: Sachs, Art. 2 Rn. 73d.