Die Strafbarkeit des Aufbaus von Botnetzen

Von Akad. Mitarbeiter Dr. **Fabian Stam**, Potsdam

I. Einleitung

Mit dem Fortschreiten der Digitalisierung zeigen sich die mit ihr verbundenen Gefahren immer deutlicher: Die Häufung sogenannter „Denial of Service"-Angriffe, mit denen durch massenweise Anfragen an Internetseiten deren Erreichbarkeit gestört wird, sowie gezielter Angriffe auf Netzwerke von Unternehmen, aber etwa auch des Deutschen Bundestags 2015, lässt erahnen, mit welchen (kriminellen oder terroristischen) Bedrohungen in Zukunft zu rechnen ist. Derartige Angriffe werden regelmäßig mit Hilfe sogenannter Botnetze ausgeführt. Der Beitrag stellt kurz die technischen Grundlagen dieser Netze dar und untersucht sodann, inwiefern der Aufbau von Botnetzen (das heißt die unerwünschte Installation eines Bot-Programms auf einem fremden Computer[1]) nach geltendem Recht strafbar ist. Zentrale Bedeutung kommt in diesem Zusammenhang der bislang kaum beachteten Frage zu, wann es sich bei einer Zugangssicherung i.S.d. § 202a StGB um eine „besondere" handelt.[2] Abschließend stellt sich die Frage, ob gesetzgeberischer Handlungsbedarf besteht.

II. Technische Grundlagen

1. Bots und Botnetze

Botnetze (von engl. robot = Roboter, wiederum von tschechisch Robota = Arbeit) sind Verbünde infizierter Computer, die von einem zentralen sog. „Command & Control-Server" ferngesteuert werden.[3] Ein Bot ist ein Computerprogramm, das vom Angreifer üblicherweise über andere Schadprogramme verbreitet wird und der Vernetzung der Computer dient. Darüber hinaus können Bots weitere – hier nicht näher untersuchte – Funktionen aufweisen, z.B. als Keylogger agieren, d.h. sämtliche Tastatureingaben des Nutzers speichern und (z.B. zwecks Identitätsdiebstahls) an einen anderen Rechner schicken.

Ziel des Aufbaus eines Botnetzes ist es, die Rechenleistung und Bandbreite tausender, hunderttausender oder gar Millionen von Computern[4] und Internetzugängen kombiniert zu nutzen.[5] Neben dem Einsatz für „Denial of Service"-Angriffe ist eine Vielzahl anderer Einsatzmöglichkeiten denkbar. So nutzten die Täter in einem jüngst vom BGH entschiedenen Fall[6] ein Botnetz, um mit Hilfe der kombinierten Rechenleistung Bitcoins – eine digitale Währung[7] – zu erzeugen. Hierfür wird der Bot auf den (dann infizierten) Computer installiert und dessen Startroutine dahingehend verändert, dass das Bot-Programm bei jedem Start unbemerkt mit ausgeführt wird. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) geht für 2016 von täglich bis zu 39.000 Neuinfektionen aus.[8]

2. Verbreitungswege von Bot-Programmen

Bot-Programme können grob gesagt über drei Wege verbreitet werden: mittels eines Trojanischen Pferds, eines Drive-By-Downloads oder eines gezielten Angriffs auf den betroffenen Rechner (Advanced Persistent Threat – APT), wobei letztere aufgrund des wesentlich höheren Aufwands deutlich seltener sind[9] und deshalb im Folgenden nicht näher untersucht werden.

a) Trojanisches Pferd

Der Begriff des Trojanischen Pferds (kurz und im Folgenden: Trojaner[10]) knüpft an die Sage vom Kampf um Troja an, in dessen Verlauf die sich scheinbar zurückziehenden Griechen

---

[1] Wenn im Folgenden von Computern gesprochen wird, umfasst dies sämtliche mit dem Internet verbundenen Geräte wie Smartphones, Tablet-PCs, Smart-TVs usw.

[2] Keine Ausführungen etwa bei *Eisele*, Strafrecht, Besonderer Teil, Bd. 1, 4. Aufl. 2017, Rn. 733 ff.; *ders.*, Computer- und Medienstrafrecht, 2013, § 6 Rn. 8 ff.; *Maurach/Schroeder/Maiwald*, Strafrecht, Besonderer Teil, Bd. 1, 10. Aufl. 2009, Rn. 92 ff.; *Krey/Heinrich/Hellmann*, Strafrecht, Besonderer Teil, Bd. 1, 15. Aufl. 2012, Rn. 609 ff.; *Hilgendorf*, in: Laufhütte/Rissing-van Saan/Tiedemann (Hrsg.), Strafgesetzbuch, Leipziger Kommentar, Bd. 6, 12. Aufl. 2010, § 202a Rn. 29 ff.; *Lenckner/Eisele*, in: Schönke/ Schröder, Strafgesetzbuch, Kommentar, 29. Aufl. 2014, § 202a Rn. 14 ff.; *Kargl*, in: Kindhäuser/Neumann/Paeffgen (Hrsg.), Nomos Kommentar, Strafgesetzbuch, Bd. 2, 4. Aufl. 2013, § 202a Rn. 9 ff.; *Graf*, in: Joecks/Miebach (Hrsg.), Münchener Kommentar zum Strafgesetzbuch, Bd. 4, 2. Aufl. 2012, § 202a Rn. 35 ff.; *Heger*, in: Lackner/Kühl, Strafgesetzbuch, Kommentar, 28. Aufl. 2014, § 202a Rn. 4; *Fischer*, Strafgesetzbuch und Nebengesetze, Kommentar, 64. Aufl. 2017, § 202a Rn. 8 ff.

[3] Bezüglich des gesamten folgenden Absatzes *Eckert*, IT-Sicherheit, 9. Aufl. 2014, S. 77-79.

[4] Das mit 30 Millionen Geräten bislang größte bekannte Botnetz war laut dem Bundesamt für Sicherheit in der Informationstechnik (Hrsg.), Die Lage der IT-Sicherheit in Deutschland 2016, 2016, S. 26, „Bredolab" im Jahr 2012.

[5] Dem Prinzip nach ganz ähnlich – jedoch mit Zustimmung des jeweiligen Computernutzers – funktioniert das sog. „Volunteer Computing", bei dem durch das Herunterladen und Ausführen eines Computerprogramms die Rechenleistung des eigenen Computers anderen zur Verfügung gestellt wird. Ein Beispiel hierfür ist das Projekt „SETI@home" (Search for Extra-Terrestrial Intelligence at home) der Universität Berkeley, das auf diese Weise bei der Suche nach außerirdischer Intelligenz unterstützt werden kann, siehe dazu https://setiathome.berkeley.edu (23.7.2017).

[6] BGH NStZ 2016, 339.

[7] Näher zu Bitcoins *Kuhlmann*, CR 2014, 691.

[8] Bundesamt für Sicherheit in der Informationstechnik (Fn. 4), S. 26.

[9] Bundesamt für Sicherheit in der Informationstechnik (Fn. 4), S. 22 f.

[10] Auch wenn es sich bei dem mythischen Holzpferd selbstverständlich nicht um einen Trojaner handelt, wird (da diese Bezeichnung inzwischen üblich ist) im Folgenden der Begriff „Trojaner" als Synonym für „Trojanisches Pferd" verwendet.

den Bewohnern Trojas ein hölzernes Pferd schenkten, in dem sich griechische Soldaten versteckt hatten, die in der Nacht aus dem Pferd kletterten und den Griechen von innen die Stadttore öffneten.[11] Es handelt sich dabei um Computerprogramme, die eine hilfreiche Funktion vortäuschen, jedoch Schadsoftware, z.B. Bot-Programme, enthalten.[12] Der Trojaner entspricht dabei dem hölzernen Pferd der Sage, das Bot-Programm den griechischen Soldaten. Trojaner können (wie auch andere Schadsoftware wie Viren und Würmer) über verschiedene Wege verbreitet werden. Häufig werden sie in zum Download angebotenen Dateien versteckt oder per E-Mail verbreitet. Letztere werden in der Regel selbst von Bot-Programmen (z.B. an alle im elektronischen Adressbuch eines infizierten Computers enthaltenen E-Mail-Adressen) versandt; die beigefügten Datei-Anhänge (z.B. Dokumente oder Bild-Dateien), zu deren Öffnen der Empfänger scheinbar von einer ihm bekannten Person aufgefordert wird, enthalten die Schadsoftware. Darüber hinaus ist eine Verbreitung über physische Datenträger (z.B. USB-Sticks oder DVDs) möglich.[13]

b) Drive-By-Downloads

Immer weitere Verbreitung finden sog. „Drive-By-Downloads" (von engl. drive-by = im Vorbeifahren).[14] Dabei lädt der Computer Schadsoftware herunter, ohne dass der Nutzer dies aktiv initiiert hat oder auch nur bemerkt. Hierfür kann bereits das Besuchen einer entsprechend präparierten bzw. infizierten (oftmals im Übrigen seriösen) Internetseite oder das Öffnen einer E-Mail genügen. Möglich ist diese Art des Angriffs durch das Ausnutzen von Schwachstellen in Browser- und anderen Programmen (insbesondere Adobe Flash Player[15]). 2015 gingen Drive-By-Angriffe laut BSI von 1-2 % aller Internetseiten in Deutschland aus (wobei hierin auch Verweisungen auf andere Seiten, insbesondere durch Werbebanner, enthalten sind).[16]

3. Schutzmöglichkeiten

Antivirenprogramme können bekannte Trojaner oder die in ihnen enthaltene Schadsoftware erkennen, bieten aufgrund der ständigen technischen Entwicklung aber keinen zuverlässigen Schutz. Von zentraler Bedeutung ist zudem vorsichtiges Verhalten des Computernutzers, indem z.B. Datei-Anhänge von unbekannten E-Mail-Absendern nicht geöffnet werden. Firewalls bieten gegen das Einschleusen von Schadsoftware keinen Schutz. Sie fungieren – stark vereinfacht – lediglich im Sinne eines Torwächters, der darüber entscheidet, welche auf dem Computer installierten Programme Internetzugriff erhalten und welche nicht.[17] Insofern kann eine restriktiv eingestellte Firewall unter Umständen verhindern, dass ein einmal installiertes Bot-Programm auf das Internet zugreift. Die Installation selbst kann sie jedoch nicht verhindern, da der Inhalt der transportierten Daten durch sie in aller Regel nicht geprüft wird.[18] Anderes mag gelten, wenn die Firewall mit einem Antiviren-Programm kombiniert wird, das alle eingehenden Daten untersucht. Den Schutz vermittelt dann jedoch in erster Linie dieses Programm, nicht hingegen die Firewall selbst. Gegen Drive-By-Downloads können allein eine restriktive Konfiguration des Internet-Browsers, die fortlaufende Software-Aktualisierung und der restriktive Umgang mit Scriptsprachen (z.B. JavaScript) schützen.[19]

III. Rechtliche Würdigung

1. Strafbarkeit nach § 202a StGB

Nach bislang wohl einhelliger Meinung soll die Installation eines Bot-Programms mittels Trojaners oder Drive-By-Downloads von 202a StGB erfasst sein.[20] Danach ist strafbar, „wer unbefugt sich oder einem anderen Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft".

a) „Zugang zu Daten verschaffen"

Einen Zugang zu Daten verschafft sich, wer in eine Position gelangt, in der er auf sie zugreifen kann.[21] Auf den tatsächlichen Zugriff kommt es dagegen nach einhelliger Meinung nicht an, während dies nach der Gesetzesfassung bis 2007 umstritten war.[22] Mit der Änderung von 2007 wollte der Gesetzgeber das schlichte Hacking, also das Eindringen in fremde Netze, ohne dass auf Daten zugegriffen wird, anders als noch bei Einführung des § 202a StGB im Jahr 1986, wo dies ausdrücklich straflos bleiben sollte,[23] von § 202a StGB erfasst wissen.[24]

[11] *Homer*, Odyssee, 8. Gesang, 492-520.
[12] *Eckert* (Fn. 3), S. 73-77.
[13] Zum technisch identischen Verbreitungsweg von Computerviren *Eckert* (Fn. 3), S. 58-65.
[14] Bezüglich des gesamten folgenden Absatzes *Eckert* (Fn. 3), S. 159.
[15] Bundesamt für Sicherheit in der Informationstechnik (Fn. 4), S. 29.
[16] Bundesamt für Sicherheit in der Informationstechnik (Hrsg.), Die Lage der IT-Sicherheit in Deutschland 2015, 2015, S. 32.
[17] Eingehend zur Technik von Firewalls *Eckert* (Fn. 3), S. 728-760.
[18] *Eckert* (Fn. 3), S. 757.
[19] *Eckert* (Fn. 3), S. 159.
[20] *Buermeyer/Golla*, K&R 2017, 14 (15); wohl auch *Mavany*, ZRP 2016, 221 (223); *ders.*, KriPoZ 2016, 106 (109); siehe ferner die Erklärung der Bundesregierung, BT-Drs. 18/10182, S. 19.
[21] *Hilgendorf* (Fn. 2), § 202a Rn. 16; *Kargl* (Fn. 2), § 202a Rn. 12; *Graf* (Fn. 2), § 202a Rn. 56; *Heger* (Fn. 2), § 202a Rn. 5; *Fischer* (Fn. 2), § 202a Rn. 10; jeweils m.w.N.
[22] Siehe zu diesem Streit *Graf* (Fn. 2), § 202a Rn. 50-55 m.w.N.
[23] BT-Drs. 10/5058, S. 28.
[24] So ausdrücklich die Entwurfsbegründung zu § 202a StGB n.F. von 2006, BT-Drs. 16/3565, S. 9.

b) „Zugangssicherung“

aa) Ausgangspunkt

Geht man davon aus, dass der Täter durch die Installation des Bot-Programms Zugriff auf den infizierten Computer und damit Zugang zu den dort gespeicherten Daten erlangt, hängt die Strafbarkeit davon ab, dass diese Daten „besonders gegen unberechtigten Zugang gesichert“ waren und der Täter diese Sicherung überwunden hat. Nach der Entwurfsbegründung von 1986 sollen „nicht alle Daten […], sondern nur diejenigen, die ‚besonders gesichert‘ sind, d.h. solche, bei denen der Verfügungsberechtigte durch seine Sicherung sein Interesse an der ‚Geheimhaltung‘ dokumentiert“ hat, dem Tatbestand unterfallen.[25] Dementsprechend liegt eine besondere Zugangssicherung vor, wenn der Berechtigte Vorkehrungen getroffen hat, die objektiv geeignet und subjektiv dazu bestimmt sind, den Zugriff auf Daten zu verhindern oder zumindest nicht unerheblich zu erschweren, wobei sich in der Sicherung sein Interesse an der Geheimhaltung (als geschütztes Rechtsgut) manifestieren muss.[26] Die bloße Manifestation, etwa durch einen Hinweis, die Daten geheim halten zu wollen, genügt hingegen nicht.[27] Der Schutz vor unbefugtem Zugriff braucht indes nicht alleiniger Zweck der Maßnahme zu sein; allgemeine Sicherungen, die die Daten lediglich reflexartig vor unbefugtem Zugang schützen, wie etwa die abgeschlossene Wohnungstür, genügen jedoch nicht.[28] Zwar wird kein hoher Sicherungsgrad (schon gar keine Unüberwindbarkeit) gefordert, eine für jeden Interessierten ohne großen Aufwand überwindbare Sicherung erfüllt die Anforderungen aber nicht.[29] Aus dem Begriff der Sicherung ergibt sich, dass sie zum Tatzeitpunkt wirklich bestehen muss.[30]

bb) Erforderliche Schutzrichtung der „Zugangssicherung“

Bislang nicht geklärt ist indes die Frage, ob lediglich irgendeine das Geheimhaltungsinteresse manifestierende Sicherung bestehen oder ob sich diese gegen die spezifische Angriffsart richten muss. Auf den ersten Blick mag erstere Deutungsweise naheliegen, da eine Sicherung gegen sämtliche Angriffsarten schlicht unmöglich ist. Dann könnte etwa der Einsatz einer Firewall eine besondere Zugangssicherung sein, obwohl sie keinen Schutz gegen die Installation eines Bot-Programms bietet. Lässt man indes auch solche Schutzmaßnahmen genügen, die zwar in gewisser Weise Schutz bieten, den konkreten Angriff aber überhaupt nicht abwehren können, reduziert man die Zugangssicherung auf einen bloß symbolischen Akt, der nach einhelliger Meinung jedoch gerade nicht genügt. Plausibler ist es daher zu fordern, dass die Zugangssicherung die Daten gerade vor Angriffen wie dem konkret vorgenommenen schützen soll.[31]

Der Einsatz von Firewalls stellt demnach grundsätzlich keine Zugangssicherung i.S.d. § 202a StGB dar.[32] Da das Risiko der Infektion durch Drive-By-Downloads lediglich durch individuelle Vorsichtsmaßnahmen verringert werden kann (oben II. 3.), handelt es sich bei einer Infektion auf diesem Weg nicht um die Überwindung einer Zugangssicherung im Sinne des § 202a StGB.[33] Dient ein Antiviren-Programm auch dem Schutz vor Trojanern und der Installation von Bots, handelt es sich dagegen hiernach um eine Zugangssicherung.[34]

cc) Das „Besondere“ der „Zugangssicherung“

§ 202a StGB lässt jedoch nicht jede, sondern allein eine besondere Zugangssicherung zur Begründung der Strafbarkeit genügen. Die Bedeutung dieses Merkmals wurde in der Literatur bislang indes kaum erörtert. Nach *Hilgendorf/Valerius* verdeutlicht das Merkmal lediglich, dass die Sicherheitsvor-

[25] BT-Drs. 10/5058, S. 29.

[26] *Lenckner/Eisele* (Fn. 2), § 202a Rn. 14; ferner *Fischer* (Fn. 2), § 202a Rn. 8; *Kargl* (Fn. 2), § 202a Rn. 9; *Graf* (Fn. 2), § 202a Rn. 32; *Heger* (Fn. 2), § 202a Rn. 4; *Hilgendorf/Valerius*, Computer- und Internetstrafrecht, 2. Aufl. 2012, Rn. 546; *Schultz*, DuD 2006, 778 (780).

[27] *Kargl* (Fn. 2), § 202a Rn. 9; *Hilgendorf* (Fn. 2), § 202a Rn. 29; *Hilgendorf/Valerius* (Fn. 26), Rn. 546; *Ernst*, NJW 2003, 3233 (3236); *Schmachtenberg*, DuD 1998, 7.

[28] *Fischer* (Fn. 2), § 202a Rn. 9; *Lenckner/Eisele* (Fn. 2), § 202a Rn. 14; *Graf* (Fn. 2), § 202a Rn. 35; *Hilgendorf* (Fn. 2), § 202a Rn. 30; *Schmitz*, JA 1995, 478 (482); *Krutisch*, Strafbarkeit des unberechtigten Zugangs zu Computerdaten und -systemen, 2004, S. 111 f.

[29] *Fischer* (Fn. 2), § 202a Rn. 9; *Lenckner/Eisele* (Fn. 2), § 202a Rn. 14; *Kargl* (Fn. 2), § 202a Rn. 9; *Graf* (Fn. 2), § 202a Rn. 32; *Hilgendorf* (Fn. 2), § 202a Rn. 32; *Hilgendorf/Valerius* (Fn. 26), Rn. 550; *Eisele* (Fn. 2 – Computer- und Medienstrafrecht), § 6 Rn. 17; *Hilgendorf*, JuS 1996, 702; *Schmachtenberg*, DuD 1998, 7. Dagegen stellt *Schultz* (DuD 2006, 778 [780]) maßgebend darauf ab, ob „der Berechtigte den Zugang zu seinen Daten dergestalt behindert, dass für den Verkehr objektiv ersichtlich ist, dass ein regulärer Zugriff vom Willen des Berechtigten abhängig sein soll“, und überbetont damit die Manifestation des entgegenstehenden Willens; der Sicherung kommt nach dieser Sichtweise gerade keine Sicherungs-, sondern lediglich eine Symbolfunktion zu.

[30] *Lenckner/Eisele* (Fn. 2), § 202a Rn. 8; *Graf* (Fn. 2), § 202a Rn. 32; *Maurach/Schroeder/Maiwald* (Fn. 2), § 29 Rn. 102; *v. Gravenreuth*, NStZ 1989, 201 (206).

[31] So wohl auch *Lenckner/Eisele* (Fn. 2), § 202a Rn. 14; *Dietrich*, Das Erfordernis der besonderen Sicherung im StGB am Beispiel des Ausspähens von Daten, § 202a StGB, 2009, S. 384.

[32] So (ohne Begründung) auch BGH NStZ 2016, 339 (340).

[33] A.A. *Buermeyer/Golla*, K&R 2017, 14 (15), die ohne weitere Begründung (entgegen dem oben Gesagten) davon ausgehen, dass es sich bei der Ausnutzung von Sicherheitslücken um die Überwindung einer Zugangssicherung handele. Das kann aber allenfalls in Bezug auf Sicherheitslücken in z.B. Virenschutzprogrammen, nicht aber bezüglich Internetbrowsern gelten.

[34] Lediglich erwähnt sei in diesem Zusammenhang, dass auf (inzwischen weit verbreiteten) Apple-Computern in der Regel überhaupt keine Antiviren-Programme installiert sind, dort also häufig schon deshalb keine Zugangssicherung vorliegen wird.

kehrung geeignet sein muss, „den Zugriff Unbefugter auszuschließen oder zumindest erheblich zu erschweren.“[35] Nach *Jessen* soll eine besondere Sicherung vorliegen, wenn „ein Außenstehender dem Rechtsgutsträger bestätigt, sorgfältig gehandelt zu haben“. Hierfür müssten die Maßnahmen „nicht dem neuesten Stand der Technik entsprechen“, sondern „nach objektiven und für alle gleichermaßen geltenden Maßstäben sorgfältig ausgesucht, installiert und betrieben werden.“[36] Gegen beide Ansätze spricht indes, dass nach ihrer Lesart das Wort „besonders“ keine eigenständige Bedeutung hat, sondern in der Zugangssicherung aufgeht. Denn eine Sicherung, die Unbefugte nicht ausschließt oder ihren Zugriff erschwert, also auch nicht sorgfältig ausgewählt wurde, ist bereits keine Sicherung, sondern allenfalls der Versuch einer Sicherung. Die Art der Sicherung entscheidet deshalb nicht darüber, ob es sich um eine besondere, sondern darüber, ob es sich überhaupt um eine Sicherung handelt.

Dem allgemeinen Sprachgebrauch entsprechend handelt es sich bei einer besonderen Zugangssicherung um ein „Mehr“ gegenüber einer allgemeinen, d.h. der Datenverfügungsberechtigte muss einen höheren als den „normalen“ Schutz herstellen. Das korrespondiert mit dem Erfordernis, dass die Zugangssicherung das Geheimhaltungsinteresse des Verfügungsberechtigten manifestieren muss. Nur wenn das Schutzniveau erhöht wird (sei es durch erstmalige Einrichtung einer Zugangssicherung oder Verbesserung einer vorhandenen), kann eine solche Manifestation und damit eine besondere Zugangssicherung angenommen werden.

Daraus folgt für den Schutz vor Bot-Programmen durch Virenscanner ein Problem: Regelmäßig ist auf neu gekauften Computern bereits ein solches Programm vorinstalliert, d.h. der Nutzer muss nichts unternehmen, um eine Zugangssicherung im Sinne des § 202a StGB einzurichten, manifestiert seinen Geheimhaltungswillen also gerade nicht. Es handelt sich deshalb in der Regel nicht um eine besondere Zugangssicherung, und § 202a StGB ist deshalb, folgt man der hiesigen Norminterpretation, in diesen Fällen nicht erfüllt. Anderes gilt in der Regel nur, wenn er das Programm selbst installiert, beim erstmaligen Einschalten gefragt wird, ob er das Programm verwenden will oder er (z.B. nach Ablauf einer Testversion) aktiv tätig wird, um den Schutz zu verlängern. Kauft der Nutzer hingegen einen Computer ohne Virenschutz und installiert das (unter Umständen identische) Antiviren-Programm selbst, liegt eine besondere Zugangssicherung dagegen unproblematisch vor. Ein Antiviren-Programm ist somit nur dann eine besondere Zugangssicherung, wenn der Nutzer aktiv dafür gesorgt hat, dass es auf dem Computer läuft. Dennoch kann eine besondere Zugangssicherung auch dann vorliegen, wenn der Nutzer einen werkseitig mit einem (u.U. besonders guten) Antiviren-Programm ausgestatteten Computer gekauft hat, zu dessen Aktivierung er nicht weiter tätig werden muss. Hat er das Gerät nämlich gerade wegen des Programms gekauft, ist bereits in dem Kauf die Manifestation des Geheimhaltungswillens bezüglich der später gespeicherten Daten zu erblicken. Hat er den Computer dagegen ohne Rücksicht auf das vorinstallierte Programm gekauft, handelt es sich bei diesem nicht um eine besondere Zugangssicherung. Hiergegen mag man einwenden, dass es widersprüchlich sei, dasselbe Computerprogramm je nach der Vorstellung des Nutzers einmal als besondere Zugangssicherung anzusehen und einmal nicht. Dies ist jedoch kein Einwand gegen die hier entwickelte Ansicht, sondern ein grundsätzlicherer gegen das dem Gesetz zugrundeliegende und von der herrschenden Meinung konsentierte Begriffsverständnis der besonderen Zugangssicherung, nach dem die Manifestation des (subjekiven) Geheimhaltungswillens erforderlich ist.

dd) Rechtspraktische Probleme

Aus diesem Erfordernis der „besonderen Zugangssicherung“ ergibt sich, dass im Strafverfahren festzustellen ist, wie ein Antiviren-Programm auf dem Computer installiert oder mit welcher Intention ein werkseitig geschützter Computer gekauft wurde, wobei eine große Zahl von Nutzern dies nach Jahren des Gebrauchs vermutlich selbst nicht mehr rekonstruieren und wiedergeben kann. Lässt sich die Frage nicht aufklären, ist in dubio pro reo davon auszugehen, dass die Software bereits vorinstalliert war und der Nutzer den Computer nicht gerade wegen der Software gekauft hat. Aber selbst wenn man nicht dem hier vertretenen Verständnis der besonderen Zugangssicherung folgen will, dürfte es regelmäßig ganz erhebliche Probleme bereiten festzustellen, ob der Virenschutz zur Zeit der Infektion überhaupt aktiv war oder (etwa infolge manuellen Ausschaltens oder eines Programmfehlers) nicht.[37]

c) Zwischenergebnis

Es zeigt sich, dass das Einschleusen von Bot-Programmen auf fremde Computer aus verschiedenen Gründen häufig nicht § 202a StGB unterfällt. Selbst wenn dies jedoch der Fall ist, stellt der Tatbestand Gerichte vor schwierige Beweisprobleme, sodass im Ergebnis ein Großteil von Taten nach dieser Vorschrift straflos bleibt.

2. Strafbarkeit nach § 303a StGB

Denkbar ist jedoch eine Strafbarkeit nach § 303a StGB, wonach sich strafbar macht, „wer rechtswidrig Daten (§ 202a Abs. 2) löscht, unterdrückt, unbrauchbar macht oder verändert“. Die Vorschrift soll nach der Entwurfsbegründung[38] und ganz herrschender Auffassung[39] als Daten dargestellte Infor-

[35] *Hilgendorf/Valerius* (Fn. 26), Rn. 550.

[36] *Jessen*, Zugangsberechtigung und besondere Sicherung im Sinne von § 202a StGB, 1994, S. 120; so auch *Krutisch* (Fn. 28), S. 109 f.

[37] Fehlende entsprechende Feststellungen bemängelt BGH NStZ 2016, 339 (340).

[38] BT-Drs. 10/5058, S. 34.

[39] *Stree/Hecker*, in: Schönke/Schröder (Fn. 2), § 303a Rn. 1; *Wieck-Noodt*, in: Joecks/Miebach (Hrsg.), Münchener Kommentar zum Strafgesetzbuch, Bd. 5, 2. Aufl. 2014, § 303a Rn. 2; *Heger* (Fn. 2), § 303a Rn. 1; *Zaczyk*, in: Kindhäuser/Neumann/Paeffgen (Hrsg.), Nomos Kommentar, Strafgesetzbuch, Bd. 3, 4. Aufl. 2013, § 303a Rn. 3; *Fischer* (Fn. 2), § 303a Rn. 2; *Krey/Hellmann/Heinrich*, Strafrecht, Besonde-

mationen gegen die Beeinträchtigung oder Beseitigung ihrer Verwendbarkeit und damit das Interesse des Berechtigten an der unversehrten Verwendbarkeit der gespeicherten Daten schützen. Davon ausgehend werden Daten verändert, wenn ihr Informationsgehalt umgestaltet wird und hierdurch die ursprüngliche Funktion und damit wiederum der ursprüngliche Verwendungszweck beeinträchtigt wird;[40] ob die Veränderung zu einer Verbesserung führt, soll dabei irrelevant sein.[41] Wird das Bot-Programm auf den Computer geschleust, werden hierdurch in der Regel Daten verändert, wird z.B. die Startroutine dahingehend geändert, dass das Bot-Programm bei jedem Start ausgeführt wird. Die unbemerkte Installation eines Bot-Programms realisiert daher in der Regel § 303a StGB.[42]

IV. Gesetzgeberischer Handlungsbedarf?

Nachdem also feststeht, dass das Einschleusen von Bot-Programmen in der Regel zwar nicht § 202a StGB unterfällt, jedoch nach § 303a StGB strafbar ist, stellt sich die Frage, ob gleichwohl gesetzgeberischer Handlungsbedarf besteht. Während dies nach Auffassung des Bundesrats der Fall ist,[43] verneint die Bundesregierung dies. So „bestehen nach Ansicht der Bundesregierung dabei jedenfalls keine gravierenden Strafbarkeitslücken. Nahezu sämtliche Aktivitäten beim Aufbau […] eines Botnetzes unterfallen bereits nach geltendem Recht Straftatbeständen des Strafgesetzbuches. […] Der Aufbau eines Botnetzes mit Hilfe von Schadprogrammen ist in aller Regel als Ausspähen von Daten (§ 202a StGB) strafbar. Soweit die Schadsoftware Daten verändert, liegt der Straftatbestand der Datenveränderung (§ 303a StGB) vor.“[44] Während nach dem oben Gesagten eine Bestrafung nach § 202a StGB in der Regel nicht erfolgen kann, ist der Bundesregierung zuzustimmen, dass eine Strafbarkeit nach § 303a StGB in der Regel vorliegen wird. Das Postulat eines gesetzgeberischen Handlungsbedarfs muss sich daher zwei naheliegenden Einwänden stellen.

1. Einwand vorrangig prozessualer und praktischer Probleme

Erstens lässt eine materiell-rechtliche Lösung (also die Schaffung eines neuen Straftatbestands) ein erhebliches Problem ungelöst. Denn eine Strafverfolgung ist in der Praxis regelmäßig überhaupt nicht oder nur mit größten Schwierigkeiten möglich. Das liegt zum einen an den von Tätern eingesetzten Verschleierungstaktiken und -techniken (z.B. durch Nutzung fremder Internetzugänge, Einsatz von Proxy-Servern, Datenverschlüsselung[45]) und daran, dass es praktisch niemals zu direkten Kontakten zwischen Tätern und Opfern kommt.[46] Zum anderen erweist sich die Verfolgung der Täter jedoch selbst dann häufig als kaum oder gar nicht durchführbar, wenn eine Identifizierung möglich ist, weil diese nicht selten aus dem (außereuropäischen) Ausland operieren, der Tätigkeit der Strafverfolgungsbehörden also neben praktischen auch rechtliche Hürden gesetzt sind. Doch darf die materiell-rechtliche Frage der Strafbarkeit einer Handlung nicht mit der formell-rechtlichen ihrer Verfolgbarkeit vermengt werden, zumal die Entdeckung der Täter nicht stets ausgeschlossen ist – wie der jüngst vom BGH entschiedene Fall zeigt.[47] Praktische Schwierigkeiten bei der Strafverfolgung stellen damit kein taugliches Argument gegen die Forderung einer materiell-rechtlichen Änderung dar.

2. Einwand symbolischer Strafrechtspolitik

Der zweite (gewichtigere) Einwand ist indes der naheliegende, die Forderung nach einem neuen Straftatbestand habe rein symbolischen Charakter. Der Begriff des symbolischen Strafrechts bezeichnet – so *Roxin* – „Strafvorschriften […], die nicht in erster Linie konkrete Schutzwirkungen entfalten, sondern die durch Bekenntnis zu bestimmten Werten oder Perhorreszierung für schädlich erachteter Haltungen der Selbstdarstellung politischer oder Weltanschaulicher Gruppen dienen sollen.“[48] Die Legitimität einer Strafvorschrift hängt danach „davon ab, ob eine Vorschrift […] auch zum realen Schutz eines friedlichen Zusammenlebens nötig ist.“[49]

Der Einwand rein symbolischen Strafrechts kann indes nur verfangen, wenn das Unrecht der Tat in dem verwirklich-

rer Teil, Bd. 2, 17. Aufl. 2015, Rn. 369; *Eisele* (Fn. 2 – BT I), Rn. 501; *Hilgendorf/Valerius* (Fn. 26), Rn. 587; *Arzt/Weber/Heinrich/Hilgendorf*, Strafrecht, Besonderer Teil, 3. Aufl. 2015, § 12 Rn. 44; BayObLG JR 1994, 476; *Hilgendorf*, JR 1994, 478; a.A. *Haft*, NStZ 1987, 10: Vermögen in seiner spezialisierten Ausprägung in Daten.

[40] *Stree/Hecker* (Fn. 39), § 303a Rn. 8; *Wieck-Noodt* (Fn. 39), § 303a Rn. 15; *Zaczyk* (Fn. 39), § 303a Rn. 10; *Fischer* (Fn. 2), 303a Rn. 12; *Hoyer*, in: Wolter (Hrsg.), Systematischer Kommentar zum Strafgesetzbuch, Bd. 6, 9. Aufl. 2016, § 303a Rn. 11; *Arzt/Weber/Heinrich/Hilgendorf* (Fn. 39), § 12 Rn. 49; *Eisele* (Fn. 2 – BT I), Rn. 506; *Wolff*, in: Laufhütte/Rissing-van Saan/Tiedemann (Hrsg.), Strafgesetzbuch, Leipziger Kommentar, Bd. 10, 12. Aufl. 2008, § 303a Rn. 27; *Hilgendorf/Valerius* (Fn. 26), Rn. 594.

[41] *Stree/Hecker* (Fn. 39), § 303a Rn. 8; *Wieck-Noodt* (Fn. 39), § 303a Rn. 15; *Zaczyk* (Fn. 39), § 303a Rn. 10; *Fischer* (Fn. 2), § 303a Rn. 12; *Hoyer* (Fn. 40), § 303a Rn. 11; *Arzt/Weber/Heinrich/Hilgendorf* (Fn. 39), § 12 Rn. 49; *Wolff* (Fn. 40), § 303a Rn. 28.

[42] So auch *Buermeyer/Golla*, K&R 2017, 14 (15); *Mavany*, KriPoZ 2016, 106 (109). Insofern liegt der Sachverhalt bei *Hilgendorf/Valerius* (Fn. 26), Rn. 597, anders, da diese von einem Programm ausgehen, dass mit dem Trojaner gemeinsam auf Veranlassung des Nutzers gestartet wird. Dann liegt tatsächlich keine Datenveränderung vor. In der Regel wird die Schadsoftware indes selbsttätig gestartet.

[43] BR-Drs. 338/16.

[44] Erklärung der Bundesregierung zum Entwurf des Bundesrats, BT-Drs. 18/10182, S. 19.

[45] Hierzu m.w.N. *Dalby*, Grundlagen der Strafverfolgung im Internet und in der Cloud, 2016, S. 234-238; ferner *Sieber*, Gutachten C zum 69. Deutschen Juristentag, 2012, C 35-39.

[46] *Buermeyer/Golla*, K&R 2017, 14 (16).

[47] BGH NStZ 2016, 339.

[48] *Roxin*, Strafrecht, Allgemeiner Teil, Bd. 1, 4. Aufl. 2006, § 2 Rn. 37.

[49] *Roxin* (Fn. 48), § 2 Rn. 39.

ten Straftatbestand bereits ausreichend zum Ausdruck kommt, es zum Schutz des beeinträchtigten Rechtsguts also keines neuen Straftatbestands bedarf. Nicht ausreichen kann dagegen der schlichte Verweis darauf, dass die Handlung bereits irgendeinen Straftatbestand erfüllt. Es ist also zunächst zu fragen, ob der Unrechtsgehalt des Einschleusens eines Bot-Programms in der Strafbarkeit nach § 303a StGB hinreichend zum Ausdruck kommt. Hierbei sind vor allem die unterschiedlichen Schutzgüter der §§ 202a ff. StGB und des § 303a StGB zu beachten: Während das geschützte Rechtsgut der §§ 202a ff. StGB nach herrschender Meinung das formelle Datengeheimnis, d.h. die Verfügungsbefugnis des Berechtigten ist,[50] schützt § 303a StGB nach herrschender Meinung das Interesse an der unversehrten Verwendbarkeit von Daten.[51] § 303a StGB umfasst also lediglich das durch die „Sachbeschädigung an Daten" verwirklichte Unrecht.

Hierin erschöpft sich das Unrecht des Aufbaus von Botnetzen jedoch nicht. Neben dem Schutzgut des § 303a StGB wird durch die Tat vielmehr auch dasjenige der §§ 202a ff. StGB – d.h. das formelle Datengeheimnis – verletzt, wobei letzteres nach geltendem Recht jedoch unberücksichtigt bleibt. Unberücksichtigt bleiben zudem die Beeinträchtigung der Sicherheit des Internetverkehrs durch die Möglichkeit (bzw. in der Regel die Absicht) des Einsatzes dieser Programme zu äußerst sozialschädlichem (bis hin zu möglicherweise terroristischem) Verhalten und die damit verbundene hinter dem Einsatz von Bot-Programmen stehende erhebliche kriminelle Energie. All dies wird durch das geltende Recht nicht erfasst – daher besteht gesetzgeberischer Handlungsbedarf. Insofern wäre die Schaffung einer neuen Strafvorschrift zwar auch symbolisch – wie auch jede andere Strafvorschrift in ihrer positiv-generalpräventiven Funktion Symbolcharakter hat[52] –, jedoch nicht nur symbolisch.[53]

V. Ausblick

Die Installation von Bot-Programmen auf fremden Computern unterfällt in der Regel lediglich § 303a StGB. Eine Strafbarkeit nach § 202a StGB scheitert dagegen in der Regel am Fehlen einer besonderen Zugangssicherung. Da § 303a StGB dem Unrechtsgehalt und den mit der Errichtung von Botnetzen einhergehenden Gefahren nicht gerecht wird, besteht gesetzgeberischer Handlungsbedarf.

Obgleich Gegenstand dieses Beitrags die Bestandsaufnahme und nicht die Ausarbeitung eines Gesetzesvorschlags sein soll, sei abschließend im Folgenden in aller Kürze eine Lösungsmöglichkeit skizziert. Der Vorschlag des Bundesrats zur Schaffung eines neuen § 202e StGB[54] erscheint zur Lösung des aufgezeigten Problems nicht sinnvoll. Zwar würde die Installation eines Bot-Programms auf einem fremdem Rechner dem Tatbestand unterfallen, doch ist der Wortlaut des Gesetzesvorschlags derart weit, dass er zu einer extremen Ausdehnung der Strafbarkeit auch auf ganz offensichtlich nicht strafwürdige Fälle führen würde.[55] Sinnvoll ist es dagegen, den Vorschlag von *Buermeyer/Golla* aufzugreifen, wonach bestraft werden soll, „wer eine Straftat vorbereitet, indem er Programmcode auf ein informationstechnisches System ohne Einwilligung des Berechtigten in der Absicht aufbringt, diesen ausführen zu lassen."[56] Dabei sollte der Strafrahmen indes nicht – wie dort gefordert – dem des § 202c StGB (bis zu zwei Jahre Freiheitsstrafe) entsprechen, sondern höher sein, da das Aufbringen des Programmcodes bereits erheblich in die Sphäre des Computernutzers eingreift und einen solchen Eingriff nicht (wie § 202c StGB) bloß vorbereitet. Insofern bietet sich eher die Orientierung an § 202a StGB (bis zu drei Jahre Freiheitsstrafe) an.

[50] Statt vieler etwa *Heger* (Fn. 2), § 202a Rn. 1, sowie § 202b Rn. 1; *Graf* (Fn. 2), § 202a Rn. 2, sowie § 202b Rn. 2; *Lenckner/Eisele* (Fn. 2), § 202a Rn. 1, sowie § 202b Rn. 1; *Kargl* (Fn. 2), § 202a Rn. 3, sowie § 202b Rn. 3; jeweils m.w.N. In Bezug auf § 202d StGB kritisch *Stam*, StV 2017, 488 (489), m.w.N. (nicht formelles Datengeheimnis, sondern gespeicherte Information).

[51] *Heger* (Fn. 2), § 303a Rn. 1; *Wieck-Noodt* (Fn. 39), § 303a Rn. 2; *Stree/Hecker* (Fn. 39), § 303a Rn. 1; *Zaczyk* (Fn. 2), § 303a Rn. 2; jeweils m.w.N.

[52] *Roxin* (Fn. 48), § 2 Rn. 37.

[53] *Hassemer*, in: Schünemann/Achenbach/Bottke/Haffke/Rudolphi (Hrsg.), Festschrift für Claus Roxin zum 70. Geburtstag am 15. Mai 2001, 2001, S. 1001 (1011), unterscheidet insofern überzeugend zwischen (nur) symbolischem und „kommunikativem" Strafrecht.

[54] BR-Drs. 338/16 – Anlage, S. 2,
„§ 202e – Unbefugte Benutzung informationstechnischer Systeme
(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.
(2) Mit Geldstrafe oder Freiheitsstrafe bis zu fünf Jahren wird bestraft, wer eine in Absatz 1 bezeichnete Handlung
1. gegen Entgelt oder
2. in der Absicht, sich oder einen Dritten zu bereichern oder einen Dritten zu schädigen,
begeht, wenn die Tat nicht in anderen Vorschriften mit schwererer Strafe bedroht ist.
[…]
(7) […]"

[55] Instruktiv und mit absurden Beispielen *Buermeyer/Golla*, K&R 2017, 14 (16 f.); ferner *Mavany*, ZRP 2016, 221 (223); kritisch zum Entwurf auch *Tassi*, DuD 2017, 175.

[56] *Buermeyer/Golla*, K&R 2017, 14 (18).