ATHENE
Nationales Forschungszentrum
für angewandte Cybersicherheit

Maßnahmen aktiver Cyberabwehr

Eine strafrechtliche und völkerrechtliche Betrachtung

Von
Alina Boll,
Tanya Gärtner,
Tim M. Hacke und
Denise Köcke

Maßnahmen aktiver Cyberabwehr

Eine strafrechtliche und völkerrechtliche Betrachtung

Impressum

Kontakt
Nationales Forschungszentrum für angewandte Cybersicherheit ATHENE
c/o Fraunhofer-Institut für Sichere Informationstechnologie SIT
Rheinstraße 75
64295, Darmstadt

Hinweise

Dieser Beitrag wurde mit Mitteln des Bundesministeriums für Bildung und Forschung (BMBF) und vom Hessischen Ministerium für Wissenschaft und Kunst (HMWK) im Rahmen ihrer gemeinsamen Förderung für das Nationale Forschungszentrum für angewandte Cybersicherheit ATHENE unterstützt.

Inhalt

1. Einleitung

Nicht zuletzt durch den russischen Angriffskrieg auf die Ukraine und eine hybride Kriegsführung auch im digitalen Raum, ist die Bedrohung durch Cyberattacken für die Wirtschaft und Politik real geworden und zeigt, dass die Gefährdungslage im Cyberraum so hoch wie nie ist.[1] Im Zuge der Digitalisierung und der damit einhergehenden digitalen Vernetzung ist die Zahl der Cyberangriffe erheblich gestiegen. So zeigt eine im Jahr 2022 durchgeführte Umfrage der Statista, dass rund 46 % der befragten Unternehmen in Deutschland mindestens einmal Opfer einer Cyberattacke wurden.[2] Mit der steigenden Zahl von Cyberangriffen geht eine steigende Zahl an erfassten Cyberstraftaten einher, die sich gegen das Internet, Datennetze, informationstechnische Systeme oder die darin verarbeiteten Daten richten.[3] Darüber hinaus haben sich die Ziele der Cyberkriminellen im Laufe der Zeit erweitert. So wurde neben kritischen Infrastrukturen, öffentlichen Einrichtungen, dem Gesundheits- und dem Bildungssektor sowie dem E-Commerce nahezu jede Branche im Jahr 2021 Opfer von Cyberangriffen.[4] Dies zeigt eindringlich, dass fast jedes Unternehmen in Deutschland Gefahr läuft, potenzielles Opfer eines Cyberangriffs zu werden.[5] Eine Erhöhung der Resilienz gegenüber Cyberangriffen und technischen Störungen muss daher eine Hauptaufgabe für alle beteiligten Akteure in Staat, Wirtschaft und Gesellschaft sein.[6]

Zur Vermeidung von Cyberangriffen, sollte die eigene IT kontinuierlich durch technische und organisatorische Maßnahmen nach dem neuesten Stand der Technik abgesichert sein.[7] Die anhaltend steigende Zahl der erfassten Cyberangriffe und Cyberstraftaten, sowie die dargestellte neue Bedrohungslage durch Cyberangriffe im Zusammenhang mit hybriden Kriegsführungen, zeigen jedoch, dass technische und organisatorische Maßnahmen zur Prävention von Cyberangriffen allein nicht mehr ausreichen. Als Ergänzung technischer und organisatorischer Präventivmaßnahmen wird vor allem das Stoppen und Verhindern von Angriffen durch Maßnahmen der aktiven Cyberabwehr diskutiert. Dabei sind unter Maßnahmen der aktiven Cyberabwehr nach *Shulman und Waidner* keinesfalls *„digitale Vergeltungsangriffe i.S.v. Hackbacks[8] oder die Cyberfähigkeit der Bundeswehr"* zu verstehen, sondern vielmehr *„technische Maßnahmen, die Angriffe stoppen oder proaktiv verhindern sollen, indem sie in die Infrastrukturen oder digitalen Ressourcen der Angreifer eingreifen"*.[9] Ziel der aktiven Cyberabwehr ist vor allem die Unterstützung der

[1] *BSI*, Die Lage der IT-Sicherheit in Deutschland, 2022, über: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2022.html?nn=129410, S. 7; *Bitkom*, Presseinformation, über: https://www.bitkom.org/Presse/Presseinformation.
[2] *Statista*, Anteil der Unternehmen, die in den letzten 12 Monaten eine Cyber-Attacke erlebt haben, in ausgewählten Ländern im Jahr 2022, über: https://de.statista.com/statistik/daten/studie/1230157/umfrage/unternehmen-die-in-den-letzten-12-monaten-eine-cyber-attacke-erlebt-haben.
[3] Unter Cybercrime-Straftaten versteht man alle Straftaten, die unter Ausnutzung der Informations- und Kommunikationstechnik (IuK) oder gegen diese begangen werden. Gemeint ist Cybercrime im engeren Sinne, dazu: https://www.bka.de/DE/UnsereAufgaben/Deliktsbereiche/Cybercrime/cybercrime_node.html.
[4] *BKA,* Cybercrime, Bundeslagebild 2021, über: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2021.html, S. 1.
[5] *Boll,* DuD 2022, 346 (346).
[6] *BSI,* Die Lage der IT-Sicherheit in Deutschland, 2022, über: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2022.html?nn=129410, S. 11.
[7] *Shulman/Waidner,* Athene Whitepaper, Aktive Cyberabwehr, 2022, über: https://www.athene-center.de/fileadmin/Downloads/aktive-cyberabwehr.pdf, S. 4; *Boll,* DuD 2022, 346 (346).
[8] Bei einem sog. Hackback handelt es sich um einen digitalen Vergeltungsschlag, der gerade nicht darauf abzielt, den unmittelbaren Angriff zu stoppen, vielmehr ist allein der Gegenschlag das Ziel.
[9] *Shulman/Waidner,* Athene Whitepaper, Aktive Cyberabwehr, 2022, über: https://www.athene-center.de/fileadmin/Downloads/aktive-cyberabwehr.pdf, S. 5.

Strafverfolgungs- und Gefahrenabwehrbehörden bei der Vereitelung und Verfolgung von Cyberangriffen.[10]

1.1 Rolle der IT-Sicherheitsforschung

Cyberangriffe bergen erhebliche Gefahren. So gehen erfolgreich durchgeführte Cyberangriffe i.d.R. mit weitreichenden finanziellen Schäden für die Angegriffenen einher. Der Branchenverband Bitkom e.V. errechnete für das Jahr 2022 allein in Deutschland Cybercrime-Schäden in Höhe von rund 203 Mrd. Euro.[11] Dies resultiert insbesondere daraus, dass Cyberangriffe zu Ausfallzeiten, Datenverlusten oder Manipulationen und in der Konsequenz zu umfassenden Serviceunterbrechungen und Produktivitätsverlusten führen.[12] Durch Cyberangriffe entstehen den Unternehmen jedoch nicht nur substanzielle Schäden wie Umsatzeinbußen, Kosten für die Wiederherstellung der Betriebssysteme, Ursachenfeststellung und Hinzuziehung von juristischen und forensischen Beratern, sondern u.U. auch Reputationsschäden.[13] Aufgrund dieser erheblichen Gefahren gilt es, Cyberangriffe schnellstmöglich zu entdecken und durch Maßnahmen der aktiven Cyberabwehr zu begegnen. Um den immer komplexer werdenden Cyberangriffen auch in Zukunft begegnen zu können, bedarf es hierzu einer *starken IT-Sicherheitsforschung*, die als unabhängige und neutral agierende Stelle – zusammen mit den Gefahrenabwehr- und Strafverfolgungsbehörden – rechtzeitig Schwachstellen, Risiken sowie stattfindende Angriffe aufzeigt und auf dessen Minimierung und Abwehr durch Maßnahmen aktiver Cybersicherheitsmaßnahmen hinwirkt.[14]

1.2 Rechtliches Risiko

Problematisch hierbei ist, dass es für IT-Sicherheitsforschende zur Durchführung aktiver Cybersicherheitsmaßnahmen zum Schutz der IT oftmals erforderlich ist, die gleichen technischen Vorgehensweisen zu nutzen, die Cyberkriminelle bei böswilligen Angriffen nutzen.[15] Trotz gänzlich anderer Zielsetzung drohen IT-Sicherheitsforschenden hieraus oftmals u.a. Haftungs- und Strafbarkeitsrisiken. Längst nicht nur vor dem Hintergrund des russischen Angriffskrieges kann eine Handlung von IT-Sicherheitsforschenden auch völkerrechtliche Implikationen und Risiken haben. Derartige rechtliche Risiken könnten wiederum die IT-Sicherheitsforschung – und somit den Schutz der Gesellschaft durch Maßnahmen zum Schutz der IT, einschließlich unserer kritischen Infrastrukturen – ausbremsen.[16]

Um die Rechtsunsicherheit auf dem Gebiet der aktiven Cyberabwehr zu reduzieren, ist es insofern dringend geboten, rechtliche Risiken der IT-Sicherheitsforschung aufzuzeigen und Empfehlungen zur Begegnung dieser ggf. bestehenden rechtlichen Risiken aufzuzeigen.

---

[10] Ebenda S. 3; *Boll,* DuD 2022, 346 (347).
[11] *Bitkom e.V.,* 203 Milliarden Euro Schaden pro Jahr durch Angriffe auf deutsche Unternehmen, über: https://www.bitkom.org/Presse/Presseinformation/Wirtschaftsschutz-2022.
[12] *Fedler*, Prefix Hijacking-Angriffe und Gegenmaßnahmen, 2012, über: https://www.net.in.tum.de/fileadmin/TUM/NET/NET-2012-08-1/NET-2012-08-1_01.pdf, S. 3.
[13] *Boll,* DuD 2022, 346 (348); *Schmidt-Versteyl*, NJW 2019, 1637 (1638); *Dittrich*, NZWiSt 2023, 8 (9).
[14] *Balaban et al*., Whitepaper zur Rechtslage der IT-Sicherheitsforschung, Version 1.0., über: https://sec4research.de/assets/Whitepaper.pdf, S. 3.
[15] *Selzer/Spiecker*, Tagesspiegel Background, Warum es einen Rechtsrahmen für die offensive Cybersicherheitsforschung braucht, 2022, über: https://background.tagesspiegel.de/cybersecurity/warum-es-einen-rechtsrahmen-fuer-die-offensive-cybersicherheitsforschung-braucht.
[16] Zur offensiven Cybersicherheitsforschung: *Boll/Selzer/Spiecker gen. Döhmann,* Tagesspiegel Background, Datenschutz in der offensiven Cybersicherheitsforschung, 2023, über: https://background.tagesspiegel.de/cybersecurity/datenschutz-in-der-offensiven-cybersicherheitsforschung; Zum Strafbarkeitsrisiko auch: *Klaas*, MMR 2022, 187 (187).

Die vorliegende Ausarbeitung möchte hierzu einen Beitrag leisten und zum einen aus Sicht des Strafrechts konkrete Vorgehensweisen der aktiven Cyberabwehr bewerten sowie zum anderen Eigenschaften von Cyberabwehrmaßnahmen im Rahmen einer völkerrechtlichen Taxonomie zu gruppieren und rechtlich einzuordnen.

2. Strafrechtliche Bewertung

Das Strafrecht definiert Regeln zum Schutz einiger unserer elementarsten Rechte (z.B. Leben, Gesundheit, Besitz). Wer diese Regeln überschreitet, muss mit Konsequenzen rechnen, die ebenfalls im Strafrecht definiert werden.

Das vorliegende Kapitel nimmt ausschließlich eine erste Einschätzung aus Sicht des deutschen Strafrechts vor. Weitere rechtliche Aspekte, die z.B. die Haftung der IT-Sicherheitsforschenden betreffen, werden nicht berücksichtigt. Es ist an dieser Stelle wichtig darauf hinzuweisen, dass eine rechtliche Bewertung der Strafbarkeit regelmäßig den individuellen Einzelfall berücksichtigen muss. Die vorliegende rechtliche Einschätzung kann eine solche individuelle Rechtsberatung nicht ersetzen.

2.1 Wiederherstellung des Internetverkehrs

Ein Ansatz der aktiven Cyberabwehr liegt in der *Wiederherstellung des ursprünglich intendierten Datenflusses des Internetverkehrs nach einem Angriff, der Einfluss auf diesen intendierten Datenfluss genommen hat*. Die Wiederherstellung des Internetverkehrs spielt vor allem bei dem *sog. BGP-Hijacking-Angriff*[17] eine Rolle, bei welchem Angreifer den Internetverkehr böswillig über oder zu den eigenen Servern umleiten.[18] Ziel des Angriffs kann insbesondere das Ausspähen und Überwachen von Daten, das Stilllegen des externen Datenverkehrs des Angegriffenen bis hin zu Man-in-the-Middle-Angriffen sein.[19] Einer der größten BGP-Hijacking-Angriffe in der Geschichte des Internets fand im April 2018 statt. In diesem Fall wurde das BGP-Protokoll von einem russischen Internetdienstanbieter manipuliert, um den Datenverkehr von rund 200 Unternehmen und Organisationen weltweit über russische Server umzuleiten. Dies führte dazu, dass Nutzer eines Webdienstes zur Verwaltung ihres Kryptogeldes zu einer gefälschten und von Hackern kontrollierten Website umgeleitet und in der Folge etwa 152.000 USD in Kryptowährung entwendet wurden.[20] Dieses Beispiel zeigt, dass sich BGP-Hijacking jederzeit wiederholen und sich mutmaßlich gegen jede Organisation und jedes Unternehmen richten kann.

[17] *Shulman/Waidner,* FAZ, Deutschlands Sicherheit – Der Weg zur aktiven Cyberabwehr, 2022, über: https://www.faz.net/pro/d-economy/cybersicherheit-der-weg-zur-aktiven-cyberabwehr-17980091.html.
[18] *Shulman/Waidner,* Athene Whitepaper, Aktive Cyberabwehr, 2022, über: https://www.athene-center.de/fileadmin/Downloads/aktive-cyberabwehr.pdf, S. 6.
[19] *Fedler*, Prefix Hijacking-Angriffe und Gegenmaßnahmen, 2012, über: https://www.net.in.tum.de/fileadmin/TUM/NET/NET-2012-08-1/NET-2012-08-1_01.pdf, S. 3.
[20] *Loshin*, BGP routing security flaw caused Amazon Route 53 incident, 2018, über: https://www.techtarget.com/searchsecurity/news/252439945/BGP-routing-security-flaw-caused-Amazon-Route-53-incident; *Goodin*, Suspicious event hijacks Amazon traffic for 2 hours, steals cryptocurrency, 2018, über: https://arstechnica.com/information-technology/2018/04/suspicious-event-hijacks-amazon-traffic-for-2-hours-steals-cryptocurrency/.

2.1.1 Technische Grundlagen

Das Internet setzt sich aus einer Reihe von Netzwerken, sogenannten *Autonomen Systemen* (AS) zusammen, die überwiegend von *Internet Service Providern* (ISP) verwaltet

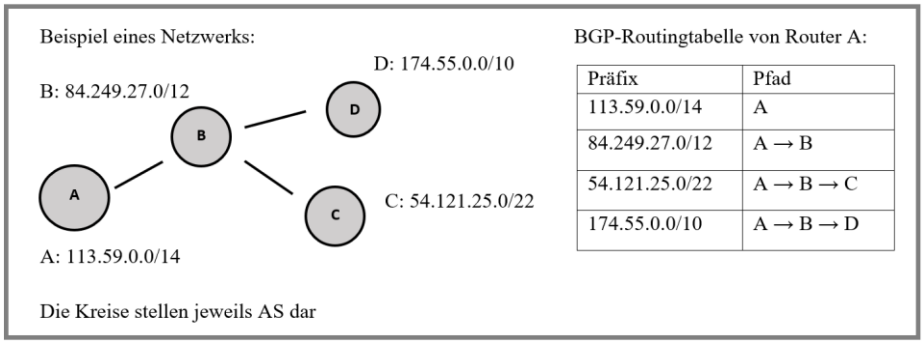

Abb. 1: Routing zwischen verschiedenen AS über BGP im Überblick[21]

und betrieben werden.[22] Dabei kontrolliert jedes AS einen oder mehrere zusammenhängende Blöcke von IP-Adressen[23], sog. *IP-Präfixe (s. auch Abb. 1)*.[24] AS können über *BGP-Router* miteinander kommunizieren und Datenverkehr (wie bspw. Nutzerdaten, Mails oder Websiteanfragen) austauschen bzw. gezielt an andere AS über ein ausgewähltes Verbindungsnetz weiterleiten, sog. *Routing*.[25] Nach den Regeln des *Border-Gateway-Protokoll (BGP)* melden alle AS die Netzwerke, mit denen sie verbunden sind und zu denen sie als Verbindungsnetz Daten weiterleiten können.[26] BGP-Router speichern dabei selbständig und kontinuierlich aktualisierend den gesamten „Postweg" (die Routen) von einem BGP-Router eines AS zu jedem BGP-Router eines anderen AS in Tabellen, *sog. BGP-Routingtabellen*.[27] Da sich die Struktur des Internets ständig ändert, neue AS hinzukommen oder andere AS nicht mehr verfügbar sind, kann jeder BGP-Router gegenüber seinen benachbarten BPG-Routern *Update-Nachrichten* (sog. Announcements) verbreiten, in welchen er mitteilt, für welches Ziel-AS (bzw. dessen Präfix) er eine effiziente Route anbieten kann.[28] Diese Update-Nachrichten werden i.d.R. von allen benachbarten BGP-Routern ohne Überprüfung ihrer Richtigkeit übernommen.[29] Einfach ausgedrückt kann man also sagen, dass es niemanden gibt, der überprüft, ob dem Postboten die richtige Wegbeschreibung zum Adressaten mitgeteilt wurde oder ob diese böswillig verändert wurde.

Bei einem BGP-Hijacking-Angriff kann der Angreifer – der einen BGP-Router kontrolliert – nun vergleichsweise einfach ganze Adressbereiche - IP-Präfixe - seiner Opfer übernehmen, indem er fälschlicherweise in einer Update-Nachricht den Besitz der IP-Präfixe seines Opfers

[21] Abbildung angelehnt an: *Fedler*, Prefix Hijacking-Angriffe und Gegenmaßnahmen, 2012, über: https://www.net.in.tum.de/fileadmin/TUM/NET/NET-2012-08-1/NET-2012-08-1_01.pdf, S. 2.
[22] *Kochheim*, Cybercrime und Strafrecht in der Informations- und Kommunikationstechnik, S. 64 Rn. 154.
[23] Eine IP-Adresse ist eine eindeutige und individuell zugeteilte Anschlussnummer eines jeden Gerätes im Internet. Die IP-Adresse identifiziert jedes Gerät im Internet, damit es adressierbar und erreichbar ist.
[24] *Kochheim*, Cybercrime und Strafrecht in der Informations- und Kommunikationstechnik, S. 850 Rn. 151 ff.
[25] Ebenda, S. 64 Rn. 151.
[26] Ebenda, S. 817 Rn.151 ff.
[27] Ebenda, S. 64 Rn. 153.
[28] Vgl. dazu: *Dierichs/Pohlmann,* c't 3/2006, 161 (162); *Shulman/Waidner*, FAZ, Deutschlands Sicherheit – Der Weg zur aktiven Cyberabwehr, 2022, über: https://www.faz.net/aktuell/wirtschaft/digitec/cybersicherheit-der-weg-zur-aktiven-cyberabwehr-17980091.html.
[29] *Fedler*, Prefix Hijacking-Angriffe und Gegenmaßnahmen, 2012, über: https://www.net.in.tum.de/fileadmin/TUM/NET/NET-2012-08-1/NET-2012-08-1_01.pdf, S. 2 ff.

behauptet.[30] Vereinfacht ausgedrückt behauptet der Angreifer, dass er die „Post-Adresse" des Opfers besitzt, sodass er in der Konsequenz dessen Briefe abfangen kann. Dies ist für den Angreifer problemlos möglich, da im BGP keine Sicherungsmaßnahmen integriert sind und allein darauf vertraut wird, dass miteinander verbundene Netzwerke die Wahrheit darüber sagen, welche IP-Adressen sie besitzen.[31] Akzeptiert ein BGP-Router die Update-Nachricht des Angreifers, hat dies zur Folge, dass er eine falsche Route lernt, diese weitergibt und dann von anderen BGP-Routern übernommen wird, wodurch in der Konsequenz der Internet-Verkehr des Opfers über manipulierte Wege umgeleitet, überwacht oder gar abgefangen und ausgespäht werden kann.[32] Als aktive Verteidigungsmaßnahme zur Abwehr des BGP-Hijacking-Angriffs kann der IT-Sicherheitsforschende nun – nachdem er einen Teil der gehijackten IP-Präfixe des Opfers kennt – eine korrigierende Update-Nachricht an einen BGP-Router senden, in welcher die IP-Präfixe des Opfers als zu diesem gehörig deklariert wird. Akzeptiert und priorisiert der BGP-Router diese Update-Nachricht[33], so ändert sich die Route des Datenverkehrs wieder zu Gunsten des Opfers. Der Datenverkehr wird folglich – ohne dass es eines Eingriffs in das Netz des Angreifers bedarf – nicht mehr über oder zum Angreifer, sondern zurück zum Opfer gelenkt, wodurch der Angriff gestoppt wird.[34] Zur Abwendung des Angriffs nutzt der IT-Sicherheitsforschende folglich die gleiche technische Vorgehensweise wie der Angreifer selbst. Zwar handelt der IT-Sicherheitsforschende in anderer Zweckrichtung, jedoch stellt sich die Frage, ob dies ein Strafbarkeitsrisiko ausschließt. Das Strafbarkeitsrisiko des IT-Sicherheitsforschende gilt es im Folgenden zu erörtern.[35]

2.1.2 Strafrechtliche Bewertung

Ein mögliches strafbares Verhalten des IT-Sicherheitsforschenden, ist das Ändern der BGP-Routingtabellen zu Gunsten des Opfers durch das Veröffentlichen einer Update-Nachricht.

2.1.2.1 Anwendbarkeit des deutschen Strafrechts

Im Rahmen der folgenden materiell-strafrechtlichen Untersuchung stellt sich zunächst die Frage, unter welchen Voraussetzungen das deutsche Strafrecht auf den geschilderten Sachverhalt anwendbar ist. Gemäß § 3 i.V.m. § 9 Abs. 1 StGB ist deutsches Strafrecht anwendbar, wenn die Tathandlung *oder* der Taterfolg in Deutschland stattfindet (Gebietsgrundsatz und Ubiquitätstheorie).[36] Veröffentlicht der IT-Sicherheitsforschende die Update-Nachricht, welche zur Veränderung der Routingtabelle des BGP-Routers führt, während er sich in Deutschland aufhält, ist somit deutsches Strafrecht anwendbar, selbst wenn sich der BGP-Router, an welchen die Update-Nachricht gesendet wird, im Ausland

[30] *Shulman/Waidner*, FAZ, Deutschlands Sicherheit - Der Weg zur aktiven Cyberabwehr, 2022, über: https://www.faz.net/aktuell/wirtschaft/digitec/cybersicherheit-der-weg-zur-aktiven-cyberabwehr-17980091.html.
[31] *Fedler*, Prefix Hijacking-Angriffe und Gegenmaßnahmen, 2012, über: https://www.net.in.tum.de/fileadmin/TUM/NET/NET-2012-08-1/NET-2012-08-1_01.pdf, S. 2.
[32] *Shulman/Waidner*, FAZ, Deutschlands Sicherheit - Der Weg zur aktiven Cyberabwehr, 2022, über: https://www.faz.net/aktuell/wirtschaft/digitec/cybersicherheit-der-weg-zur-aktiven-cyberabwehr-17980091.html.
[33] Eine Priorisierung wird i.d.R. durch die Verwendung einer präziseren IP-Präfix erreicht, sog. Longest Prefix Match-Regel, vgl.: *Huawei Technologies Co.,* Data Communications and Network Technologies, 2023, S. 173.
[34] *Shulman/Waidner*, FAZ, Deutschlands Sicherheit - Der Weg zur aktiven Cyberabwehr, 2022, über: https://www.faz.net/aktuell/wirtschaft/digitec/cybersicherheit-der-weg-zur-aktiven-cyberabwehr-17980091.html.
[35] Im Wesentlichen übernommen aus: *Boll,* DuD 2022, 346 (347).
[36] *Fischer*, StGB, 2023, § 3 Rn. 1, § 9 Rn. 1 ff.

befindet, weil die Tathandlung (i.S.d § 9 Abs. 1, 1. Fall StGB) auf deutschem Staatsgebiet begangen wurde.[37]

2.1.2.2 Datenveränderung, § 303 a Abs. 1 StGB

Eine Strafbarkeit des IT-Sicherheitsforschenden könnte sich zunächst aus § 303 a Abs. 1 StGB ergeben. Hiernach macht sich strafbar, wer rechtswidrig Daten i.S.d. § 202 a StGB löscht, unterdrückt, unbrauchbar macht oder verändert.

2.1.2.2.1 Tatobjekt: gespeicherte Daten i.S.d. § 202 a StGB

Tatobjekt des § 303 a Abs. 1 StGB sind *Daten* i.S.d. § 202 a StGB. Nach § 202 a Abs. 2 StGB sind zunächst nur solche Daten geschützt, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden.[38] Dabei wurde der Begriff der Daten durch den Gesetzgeber nicht näher definiert.[39] Die Legaldefinition in Abs. 2 dient nur der Einschränkung des in § 202 a Abs. 1 StGB vorausgesetzten allgemeinen Datenbegriffs. Nach h. M. ist allerdings von einem weit verstandenen Datenbegriff auszugehen, weshalb unter Daten i.S.d. § 202 a StGB *„codierte Informationen jeder Art"* zu verstehen sind.[40] Geschützt werden auch Daten, die – wie hier –offen bzw. frei verfügbar sind, bspw. im öffentlichen Internet.[41] Daten sind i.S.d. § 202 a Abs. 1 StGB *gespeichert*, wenn sie zum Zweck ihrer weiteren Verwendung erfasst, aufgenommen oder aufbewahrt sind, womit alle Formen der Verkörperung auf einem Datenträger geschützt sind.[42] Die Informationen der BGP-Routingtabellen, die durch die Update-Nachricht des IT-Sicherheitsforschenden geändert werden, lassen sich unter diesen Datenbegriff subsumieren. Diese sind zum Zweck der Konnexität und Effizienz des Internetverkehrs auf den BGP-Routern gespeichert, sodass es sich bei den BGP-Routingdaten in der Konsequenz um gespeicherte Daten i.S.d. §§ 202 a Abs. 1, 303 a Abs. 1 StGB handelt.

2.1.2.2.2 Tathandlung

Eine Strafbarkeit nach § 303 a I StGB setzt als Tathandlung eine irgendwie geartete Umgestaltung bestehender Datenbestände, d. h. - nach dem Wortlaut der Norm - eine Löschung, Unterdrückung, Unbrauchbarmachung oder Veränderung von Daten, voraus.[43] In dem hier diskutierten Fall kommt als Tathandlung die *Veränderung von Daten* in Betracht, worunter jede mögliche Form des inhaltlichen Umgestaltens gespeicherter Daten fällt, die eine Bedeutungsveränderung der Daten in ihrem Informationsgehalt oder Aussagewert und somit eine Funktionsbeeinträchtigung zur Folge hat.[44] Der Begriff ist neutral zu definieren, womit er unabhängig von der Beurteilung ist, ob die Veränderung eine Verschlechterung oder – wie hier – eine Verbesserung/Richtigstellung des Programms zur Folge hat.[45] Im Rahmen der Verteidigungsmaßnahme veröffentlicht der IT-

[37] *Fischer*, StGB, 2023, § 9 Rn. 5b; *Derksen,* NJW 1997, 1880; *Canradi/Schlömer,* NStZ 1966, 368.
[38] *Graf,* in: MüKoStGB, StGB, 2021, § 202a Rn. 10.
[39] BT-Drs. 10/5058, S. 29; kritisch hierzu und „Nachbesserungsbedarf" anmeldend: *Hilgendorf*, ZStW 2002, 650 (656); ebenso: *Scheffler/Dressel*, ZRP 2000, 514 (516).
[40] Dazu: *Graf,* in: MüKoStGB, StGB, 2021, § 202a Rn. 12; *Binder,* Strafbarkeit intelligenten Ausspähens von programmrelevanten DV-Informationen, 1994, S. 41; *Lenckner/Eisele/Winkelbauer,* CR 1986, 483 (484); *Eisele,* in: Schönke/Schröder, StGB, 2019, § 202a Rn. 3; a.A. *v. Gravenreuth*, NStZ 1989, 201 (206).
[41] Anders bei § 203 StGB oder § 23 GeschGehG; *Möhrenschlager*, wistra 1986, 128 (140); *Eisele,* in: Schönke/Schröder, StGB, 2019, § 202a Rn. 3; *Graf,* in: MüKoStGB, StGB, 2021, § 202a Rn. 12.
[42] *Eisele,* in: Schönke/Schröder, StGB, 2019, § 202a Rn. 14.
[43] *Wieck-Noodt,* in: MüKoStGB, StGB, 2022, § 303a Rn. 11 ff.
[44] *Hecker,* in: Schönke/Schröder, StGB, 2019, § 303a Rn. 8.
[45] *Lenckner/Winkelbauer,* CR 1986, 824 (829); *Möhrenschlager,* wistra 1986, 128 (141).

Sicherheitsforschende eine Update-Nachricht, in welcher er angibt, dass das IP-Präfix des Angegriffenen zu diesem gehört. In der Konsequenz ändert sich die dynamische Routingtabelle des BGP-Router zu Gunsten des Angegriffenen. Der IT-Sicherheitsforschende verändert folglich einen bestehenden Datenbestand und erfüllt somit die vom Tatbestand der Norm geforderte Tathandlung.

2.1.2.2.3 Fremdheit der Daten

Das Erfordernis der *Fremdheit der Daten* ergibt sich zwar nicht aus dem Wortlaut der Norm, um den Anwendungsbereich der Norm einzuschränken ist § 303 a Abs. 1 StGB jedoch restriktiv auszulegen und eine solche zu fordern.[46] Der Tatbestand setzt damit nach h. M. zunächst den Eingriff in *fremde Datenverfügungsbefugnisse* voraus, denn strafwürdiges Unrecht liegt nur dann vor, wenn ein anderer als der Handelnde von der Tathandlung betroffen ist, also eine *fremde Rechtsposition* verletzt wird.[47] Folglich ist zunächst zu erörtern, wer die Verfügungsbefugnis über die (Informationen auf den) BGP-Routentabellen innehat, die von dem IT-Sicherheitsforschenden durch die veröffentlichte Update-Nachricht geändert werden. Wie die Verfügungsbefugnis zu bestimmen ist, ist in Rspr. und Lit. höchst umstritten. Dies folgt aus dem Umstand, dass es – anders als beim sachenrechtlichen Begriff der Fremdheit bspw. in §§ 303, 242 StGB – an einer eindeutigen Regelung der Verfügungsbefugnis über Daten fehlt. Einer *Ansicht* zufolge lässt sich die Datenverfügungsbefugnis daraus ermitteln, auf wen sich die Daten inhaltlich beziehen.[48] Nach dieser Ansicht hat der Angegriffene die Verfügungsbefugnis über die Routen-Daten inne, denn aus dieser Information ergibt sich, dass die gehijackte IP-Präfix ihm zuzuordnen ist bzw. der Datenverkehr zu ihm geroutet werden muss. Diese Ansicht ist jedoch abzulehnen, so handelt es sich hierbei nur um einen Eingriff in das (mittelbare) rechtliche Interesse des vom Dateninhalts Betroffenen, eine Datenverfügungsbefugnis dessen ergibt sich aus dem Dateninhalt jedoch nicht.[49] Eine in der *Lit. vertretene Ansicht* begründet die Verfügungsbefugnis mit der sachenrechtlichen Zuordnung an dem Datenträger.[50] Verfügungsbefugt ist nach dieser Ansicht der Eigentümer des Datenträgers, denn dieser hat an seinen von ihm auf seinem Datenträger gespeicherten Daten Verfügungsrechte aus dinglichem Recht.[51] Die Routentabellen befinden sich auf den BGP-Routern der jeweiligen AS.[52] Geht man davon aus, dass diese AS zumeist von ISP betrieben und verwaltet werden, steht die jeweilige Verfügungsbefugnis über diese Datenträger – und folglich den Routentabellen – vordergründig dem jeweiligen ISP zu, dessen Routentabelle durch den IT-Sicherheitsforschenden geändert wurde. Steht dem IT-Sicherheitsforschenden also kein von dem ISP eingeräumtes Nutzungs- oder Zugriffsrecht zu, so sind die auf dem täterfremden Speichermedium befindlichen Routentabellen nach dieser Ansicht unproblematisch fremd i.S.d. Norm. Dieses Ergebnis geht mit der überzeugenden *Ansicht der Rspr.* einher, welche zur Ermittlung der Datenverfügungsbefugnis auf die erstmalige Datenspeicherung als den Akt der Erschaffung abstellt.[53] Hiernach ist Berechtigter i.d.R. die Stelle, auf deren Veranlassung die Speicherung erfolgt *(sog. Erstskribent).*[54] Auch hiernach steht die Verfügungsbefugnis dem jeweilige ISP zu, der die „Erschaffung" und Speicherung der

[46] *Fischer*, StGB, 2023, § 303a Rn. 4 f.; OLG Nürnberg, StV 2014, 296; *Hecker,* in: Schönke/Schröder, StGB, 2019, § 303a Rn. 3; *Zaczyk,* in: NK-StGB, StGB, Stand 2010, § 303a Rn. 4 f.
[47] *Hilgendorf/Frank/Valerius*, Computer- und Internetstrafrecht, 2005, Rn. 588; *Hecke*r, in: Schönke/Schröder, StGB, 2019, § 303a Rn. 3; zur Verfassungswidrigkeit: *Zaczyk,* in: NK-StGB, StGB, Stand 2010, § 303a Rn. 4.
[48] Zum Streit siehe: *Grützmacher,* CR 2016, 485 (490) m.w.N.
[49] So auch: *Fischer*, StGB, 2023, § 303a Rn. 4b.
[50] *Fischer*, StGB, 2023, § 303a Rn. 5; *Heger,* in: Lackner/Kühl, StGB, 2023, § 303a Rn. 4*; Hoyer,* in: SK-StGB, StGB, 2023, § 303a Rn. 5.
[51] *Wieck-Noodt,* in: MüKoStGB, StGB, 2022, § 303a Rn. 10.
[52] *Dierichs/Pohlmann,* c't 3/2006, 161 (162).
[53] So auch: *Fischer,* StGB, 2023, § 303a Rn. 4a.
[54] Vgl. BGH, Beschl. v. 27.07.2017 – 1 StR 412/16, Rn. 32; BayObLG, Urt. v. 24.06.1993 – 5St RR 5/93, Rn. 24; *Graf* in MüKoStGB, StGB, 2021, § 202a Rn. 21; *Fischer*, StGB, 2023, § 202a Rn. 7a; *Eisele,* in: Schönke/Schröder, StGB, 2019, § 202a Rn. 9.

Routingtabellen regelmäßig initiiert hat.[55] Im Ergebnis lässt sich feststellen, dass die Routentabellen und die darauf befindlichen Informationen für den IT-Sicherheitsforschenden regelmäßig fremd i.S.d. Norm sind, denn andere Personen – insbesondere die jeweilige ISP – haben das Verfügungsrecht über die Routentabellen inne.

2.1.2.2.4 Rechtswidrigkeit als Tatbestandsmerkmal

Zu diskutieren ist, ob das Verhalten des IT-Sicherheitsforschenden als *sozialadäquat* gesehen werden kann. Dies würde dazu führen, dass das Verhalten des IT-Sicherheitsforschenden zwar äußerlich den Tatbestand erfüllt, jedoch kein tatbestandsmäßiges Unrecht vorliegt und folglich eine Strafbarkeit nach § 303 a StGB ausgeschlossen wäre.[56] Der Gedanke der Sozialadäquanz wurde für Fälle entwickelt, in denen sich eine tatbestandsmäßige Handlung im Rahmen der Rechtsordnung hält.[57] Von einer Sozialadäquanz wäre vorliegend auszugehen, wenn das oben beschriebene Vorgehen des IT-Sicherheitsforschenden ohne Beanstandung üblich geworden ist.[58] Von einer solchen Üblichkeit kann im vorliegenden Fall der Abwendung eines BGP-Hijacking-Angriffs jedoch nicht die Rede sein, so legen die meisten IT-Sicherheitsforschenden ihre Vorgehensweisen zumeist erst gar nicht offen, wenn diese mit Strafbarkeits- und Haftungsrisiken verbunden sind, sodass von „Üblichsein" nicht die Rede sein kann.[59] Darüber hinaus scheint es schwer zu bestimmen, welche Formen des Systemzugriffs durch IT-Sicherheitsforschende als von der Allgemeinheit gebilligt und folglich im Rahmen der sozialen Handlungsfreiheit liegend, anzusehen sind. Zwar kommt IT-Sicherheitsforschenden bei der Gewährleistung der IT-Sicherheit eine unsagbar wichtige Rolle zu, dies allein kann es jedoch nicht rechtfertigen, dass IT-Sicherheitsforschenden das Recht zukommt, sich (stets straffrei) Zugang zu fremden IT-Systemen zu verschaffen. Vielmehr könnte es die Gefahr mit sich bringen, dass Forschungsinteressen als Vorwand missbraucht würden, um in fremde IT-Systeme einzudringen und Daten zweckentfremdet zu verarbeiten.[60]

Rechtswidrig ist das Verändern der Daten jedoch nur dann, wenn es ohne oder gegen den Willen des Verfügungsberechtigten vorgenommen wurde.[61] Folglich kann das *Einverständnis* des „Berechtigten" den Tatbestand des § 303 a StGB ausschließen.[62] Eine Strafbarkeit des IT-Sicherheitsforschenden kann daher vermieden werden, wenn der an den Daten Verfügungsberechtigte *vor* dem Stattfinden der Verteidigungsmaßnahme sein (tatbestandsausschließendes) Einverständnis erklärt, indem er der Änderung der BGP-Routingtabelle zustimmt. Rechtsunsicherheiten entstehen hier wiederum durch die Frage, wer der „Berechtigte" ist, dessen Einverständnis einzuholen ist. Der schon oben dargestellte Streit führt auch an diesem Punkt zur großen Unsicherheit in der Praxis, denn um eine Strafbarkeit von IT-Sicherheitsforschenden zu vermeiden, muss die Datenverfügungsbefugnis *eindeutig* festgestellt werden. Aufgrund der Komplexität von IT-Systemen und damit einhergehend der Verhältnisse der Berechtigung an diesen Systemen ist es teilweise nur mit großem Aufwand möglich, rechtssicher festzustellen, wer die Datenverfügungsbefugnis innehat. Demgegenüber ist dieser große organisatorische

[55] Das BGP-Protokoll ist ein offener Standard, der von der Internet Engineering Task Force entwickelt und gepflegt wurde. Es steht allen ISP zur Verfügung, um es in ihren Netzwerken zu implementieren und zu verwenden. Jedes AS und damit jeder ISP ist somit für die Implementierung und Verwaltung des BGP-Protokolls bzw. seiner Netzwerkressourcen und die Weiterleitung des Datenverkehrs in seinem Netzwerk selbst verantwortlich.
[56] Nach der h. M. und der Rspr. führt ein sozialadäquates Verhalten zu einen Tatbestandausschluss, vgl.: *Hirsch,* ZStW 74, (78); *Roxin,* in: FS Klug, 1983, S. 303; *Küpper,* GA 1987, 388; *Hassemer,* wistra 1995, 46 (81); OLG München NJW 1966, 2406; NStZ 1985, 550; BGHSt 19, 154.
[57] *Fischer*, StGB, 2023, vor § 32 Rn. 12.
[58] Vgl. zur Üblichkeit: OLG Karlsruhe, Urt. v. 26.10.1979 - 10 U 272/78.
[59] *Wagner*, PinG 2020, 66 (69).
[60] *Golla,* JZ 2021, 985 (987).
[61] *Borges/Schwenk/Stuckenberg/Wegener,* Identitätsdiebstahl und Identitätsmissbrauch im Internet, 2011, S. 234.
[62] *Wieck-Noodt,* in: MüKoStGB, StGB, 2022, § 303a Rn. 17; *Fischer*, StGB, 2023, § 303a Rn. 8.

Aufwand jedoch für sich genommen noch kein Grund, ohne Einverständnis auf fremde IT-Systeme einzugreifen.[63] Es empfiehlt sich deshalb, sowohl das Einverständnis des ISP, auf dessen BGP-Router Veränderungen vorgenommen werden, als auch das des Angegriffenen einzuholen, um eine Strafbarkeit des IT-Sicherheitsforschenden bestmöglich zu verhindern.[64] Notwendig ist eine engen Zusammenarbeit zwischen IT-Sicherheitsforschenden, ISP und dem Angegriffenen, welche mit der Verteidigungshandlung jedoch regelmäßig einverstanden sein werden, da das ursprünglich intendierte Routing durch die Maßnahme wiederhergestellt und der IP-Hijacking Angriff gestoppt wird. In der Praxis steht dem jedoch die Eilbedürftigkeit bei der Abwendung eines Cyberangriffs entgegen, dieses Problem soll im Rahmen der „mutmaßlichen Einwilligung" näher aufgegriffen werden (s. Kapitel f).

2.1.2.2.5 Subjektiver Tatbestand

Eine Strafbarkeit des IT-Sicherheitsforschende nach § 303 a StGB setzt voraus, dass dieser bezüglich der Verwirklichung des Tatbestandes zumindest bedingt vorsätzlich gehandelt hat. Bedingt vorsätzlich handelt, wer die Tatbestandsverwirklichung für möglich hält (kognitives Element) und den Eintritt des Erfolgs billigend in Kauf nimmt (voluntatives Element).[65] Ein vorsätzliches Handeln des IT-Sicherheitsforschenden ist in dem hier beschriebenen Szenario i.d.R. anzunehmen, denn dieser handelt regelmäßig mit dem notwendigen Wissen und der Intention, dass durch sein Verhalten Routing-Informationen geändert werden, die ihm nicht ausschließlich zur Verfügung stehen. Jedenfalls ist nicht auszuschließen, dass der IT-Sicherheitsforschende im Einzelfall die Änderung von fremden Daten ernsthaft für möglich hält und billigend in Kauf nimmt, womit ein jedenfalls bedingt vorsätzliches Handeln zu bejahen ist.

2.1.2.2.6 Rechtswidrigkeit

Ferner stellt sich die Frage, ob in dem hier diskutierten Szenario Rechtfertigungsgründe vorliegen, die eine Strafbarkeit des IT-Sicherheitsforschenden ausscheiden lassen. Als strafbarkeitsausschließender Rechtfertigungsgrund kommt zunächst die *mutmaßliche Einwilligung* des über die Daten Verfügungsbefugten in Betracht.[66] Es ist davon auszugehen, dass es dem mutmaßlichen Willen des Verfügungsbefugten entspricht, einen Eingriff in seine BGP-Routendaten hinzunehmen, wenn dadurch – wie vorliegend der Fall – ein höherwertiges Gut gerettet oder eine größere Gefahr abgewendet wird.[67] Die Änderung der Routingtabelle und die daraus folgenden Umlenkung des Internetverkehrs bringt den ordnungsgemäßen Zustand zurück und wahrt das Recht des Angegriffenen auf informationelle Selbstbestimmung.

Es muss jedoch beachtet werden, dass eine mutmaßliche Einwilligung nach dem Subsidiaritätsprinzip nur dann eingreift, wenn eine ausdrückliche Erklärung des Berechtigten wegen unüberwindbarer oder nur mit unverhältnismäßigen Mitteln zu überwindender Hindernisse nicht rechtzeitig eingeholt werden kann.[68] Wie unter II. 4 diskutiert, ist das Einholen einer Einwilligung im vorliegenden Fall zwar möglich aber

[63] *Golla*, JZ 2021, 985 (987).
[64] Auch wenn das tatbestandsausschließende Einverständnis schon bei innerer Zustimmung des Opfers wirksam ist und eine Zustimmungserklärung somit grundsätzlich entbehrlich wäre, vgl. dazu: *Schlehofer* in MüKoStGB, StGB, 2020, vor § 32 Rn. 177.
[65] *Fischer,* StGB, 2023, § 15 Rn. 11 f.
[66] Das Merkmal der Rechtswidrigkeit i.R.d. § 303 a StGB ist in seiner Bedeutung umstritten, folgt man der Ansicht, dass es sich bei diesem, wie bei § 303 StGB um ein allg. Deliktsmerkmal handelt, kommt daneben auch die mutmaßliche Einwilligung als Rechtfertigungsgrund in Betracht, vgl. *Fischer,* StGB, 2023, § 303a Rn. 13; *Hecker,* in: Schönke/Schröder, StGB, 2019, § 303a Rn. 10.
[67] *Joecks/Jäger*, StGB, 2021, vor § 32 Rn. 41.
[68] Zum Subsidiaritätsprinzip: *Schlehofer,* in: MüKoStGB, StGB, 2020, vor § 32 Rn. 205.

organisatorisch aufwendig und zeitintensiv. Hinzu kommt, dass es aufgrund der mannigfaltigen Rechtunsicherheiten bzgl. der in § 303 a StGB geforderten Verfügungsbefugnis bzw. des Tatbestandsmerkmals „unbefugt/fremd", sowie der umstrittenen Einordnung dessen als Rechtfertigungs- oder Tatbestandsausschließungsgrund, in der Praxis nahezu unmöglich sein wird, das Einverständnis des Verfügungsbefugten rechtzeitig und rechtsicher einzuholen. So ist es für Maßnahmen der aktiven Cyberabwehr i.d.R. dringend erforderlich, dass diese schnellstmöglich durchgeführt werden, um schwerwiegende Auswirkungen der Cyberangriffen (wie z.B. großflächige Identitätsdiebstahle) erfolgreich zu verhindern, bzw. schnellstmöglich stoppen zu können. Hinzu kommt, dass ISP regelmäßig ihren Sitz nicht ausschließlich in Deutschland haben, vielmehr gibt es auch große Anbieter in u.a. den USA und Asien, sodass es Zeitverschiebungen nur schwer möglich machen, den Verfügungsbefugten schnell genug zu erreichen und eine Einwilligung einzuholen. Darüber hinaus ist es ebenso zeitaufwendig innerhalb der jeweiligen Verfügungsbefugten Organisationen die für die Erteilung der Einwilligung verantwortliche Person ausfindig zu machen. Das Einholen einer ausdrücklichen Erklärung des Berechtigten ist folglich mit dem Sinn und Zweck der aktiven Cyberabwehr kaum vereinbar und praxisfern. Das Vorliegen einer mutmaßlichen Einwilligung des Verfügungsbefugten sollte daher in dem hier besprochenen Szenario des BGP-Hijacking angenommen werden können, womit eine Strafbarkeit des IT-Sicherheitsforschenden gem. § 303a StGB entfallen würde.

Eine andere Möglichkeit der Rechtfertigung könnte das Eingreifen des *rechtfertigenden Notstandes gem. § 34 StGB* sein.[69] Danach handelt gerechtfertigt, wer in einer gegenwärtigen, nicht anders abwendbaren Gefahr für Leben, Leib, Freiheit, Ehre, Eigentum oder ein anderes Rechtsgut eine Tat begeht, um die Gefahr von sich oder einem anderen abzuwenden, wenn bei Abwägung der widerstreitenden Interessen, namentlich der betroffenen Rechtsgüter und des Grades der ihnen drohenden Gefahren, das geschützte Interesse das beeinträchtigte wesentlich überwiegt.[70] Eine gegenwärtige und nicht anders abwendbare Gefahr für das überwiegende Rechtsgut der informationellen Selbstbestimmung sowie das Recht auf Integrität und Vertraulichkeit informationstechnischer Systeme, liegt in der unberechtigten Änderung der BGP-Routentabellen durch das Veröffentlichen einer falschen Update-Nachricht durch den Angreifer.[71] Übergeordnetes Ziel der Verteidigungsmaßnahme ist es die Daten vor einem unberechtigten Zugriff zu schützen bzw. die Funktionsfähigkeit des Routingsystems wiederherzustellen. Die konkret ergriffene Maßnahme muss hierfür erforderlich, d. h. geeignet und das relativ mildeste Mittel sein. Dabei stellt die konkrete Maßnahme das relativ mildeste Mittel dar, wenn kein gleich geeignetes, aber weniger eingriffsintensives Vorgehen existiert.[72] Die beschriebene Verteidigungsmaßnahme ist ein geeignetes Mittel, da sie den Angriff stoppt. Die Notstandshandlung muss darüber hinaus als mildestes Mittel den einzigen und letzten Ausweg aus der Notlage bilden.[73] Soweit zeitlich möglich, muss der IT-Sicherheitsforschende demnach zunächst die Hilfe staatlicher Stellen in Anspruch nehmen. Bei privaten IT-Sicherheitsforschenden ist hier stets zu prüfen, ob in dieser Situation eine Meldung an das BSI (§ 4 b Abs. 1, 2 BSIG) ein geeigneteres oder aber ein gleich geeignetes, aber milderes Mittel ist.[74] Aufgrund der Tatsache, dass sich der Angreifer bei einem BGP-Hijacking-Angriff regelmäßig bereits den vollen Zugang zum Datenverkehr des Angegriffenen verschafft hat, dieser einerseits vom Internetverkehr gänzlich abgeschnitten ist und andererseits der Gefahr des Missbrauches seiner Daten ausgesetzt

[69] Eine Rechtfertigung über die Notwehr, § 32 StGB scheidet aus, da die Verteidigungsmaßnahme hier gerade nicht gegenüber dem Angreifer (durch einen Eingriff in seine Server) erfolgt, sondern gegenüber einen „unbeteiligten Dritten". Die Verteidigungshandlung i.R.d. § 32 StGB darf sich grundsätzlich nur gegen den Angreifer selbst und dessen Rechtsgüter, nicht aber gegen Rechtsgüter unbeteiligter Dritter oder gar der Allgemeinheit richten, vgl. BGHSt 5, 245 (245 ff.).
[70] Vgl. § 34 StGB
[71] OLG Düsseldorf, Beschl. v. 15.10.1993, Rn. 5 ff.; *Ronellenfitsch,* DuD 2008, 110 (111).
[72] *Fischer*, StGB, 2023, § 34 Rn. 10; *Perron,* in: Schönke/Schröder, StGB, 2019, § 34 Rn. 18 ff.
[73] *Kühl,* in: Lackner/Kühl, StGB, 2023, § 34 Rn. 3.
[74] *Fischer*, StGB, 2023, § 34 Rn. 9a; *Wagner*, PinG 2020, 66 (73).

ist, scheint es hier jedoch unzumutbar, vorerst die Hilfe staatlicher Stellen in Anspruch zu nehmen. Die Verteidigungsmaßnahme ist somit ein geeignetes und das mildeste Mittel. Die Verteidigungshandlung wäre somit regelmäßig gerechtfertigt, sodass eine Strafbarkeit des IT-Sicherheitsforschenden auch hierdurch ausscheiden könnte.

2.1.2.2.7 Zwischenfazit § 303 a StGB

Eine Strafbarkeit des IT-Sicherheitsforschenden gem. § 303 a StGB – bei der Abwehr eines BGP-Hijacking-Angriffs – kann nach der hier vertretenen Meinung i.d.R. durch das Einholen eines Einverständnisses bzw. über das Institut der mutmaßlichen Einwilligung des Verfügungsbefugten verhindert werden. Spätestens ergibt sich ein Ausschluss der Strafbarkeit nach der hier vertretenen Meinung über den rechtfertigenden Notstand. Darüber hinaus würde eine Straftat nur dann verfolgt werden, wenn durch den Verfügungsbefugten ein *Strafantrag gem. § 303 c StGB* gestellt wurde.

2.1.2.3 Ausspähen von Daten, § 202 a Abs. 1 StGB

Eine weitere mögliche Strafbarkeit des IT-Sicherheitsforschenden aus § 202 a StGB scheidet in dem hier beschriebenen Fall regelmäßig aus. Hiernach wird bestraft, wer sich oder einem Dritten unbefugt Zugang zu Daten verschafft, die nicht für ihn bestimmt und gegen unberechtigten Zugang besonders gesichert sind. Fraglich ist, ob sich der IT-Sicherheitsforscher bei der Verteidigungsmaßnahme unbefugt Zugang zu den BGP-Routentabellen verschafft. Zur Vermeidung einer uferlosen Auslegung dieser Strafvorschrift unterliegt auch der Tatbestand des § 202 a Abs. 1 StGB einer restriktiven Einschränkung: Geschützt werden nur solche Daten, die *nicht für den Täter bestimmt* und *gegen unberechtigten Zugang besonders gesichert* sind.[75] Für eine Strafbarkeit müssten die Routentabellen gegen unberechtigten Zugang besonders gesichert sein bspw. durch Passwörter, Hardware-Sicherungen oder biometrische Zugangsverfahren.[76] Das BGP wurde jedoch ohne Mechanismen, die die Authentizität, Integrität und Vertraulichkeit von übermittelten Informationen sicherstellen, entwickelt.[77] Der IT-Sicherheitsforschende kann also ohne Überwindung von Sicherheitsmechanismen jedes Präfix als zu sich gehörend erklären und sich somit als das für das Präfix autoritativ ausgeben. Eine Authentizitätsüberprüfung findet gerade nicht statt. Eine Strafbarkeit des IT-Sicherheitsforschenden nach § 202 a Abs. 1 StGB scheitert also nach der hier vertretenen Meinung an der erforderlichen Sicherung des BGP.

2.1.2.4 Abfangen von Daten, § 202 b StGB

Ebenso kann in dem hier vorgestellten Szenario eine Strafbarkeit des IT-Sicherheitsforschenden nach § 202 b StGB nach der hier vertretenen Meinung regelmäßig ausgeschlossen werden. Gemäß § 202 b StGB macht sich strafbar, wer unbefugt Daten abfängt. Geschützt werden nicht öffentliche Daten, die sich in einem Übermittlungsvorgang befinden.[78] Bei der Beeinflussung der Routingtabellen auf BGP-Routern handelt es sich jedoch nicht um „fließenden Datenverkehr", der *abgefangen* wird. Vielmehr wird die dynamische Routingtabelle der BGP-Router durch das Veröffentlichen der Update-Nachricht *verändert*.

[75] BT-Drs. 16/3656, S. 10.
[76] *Fischer*, StGB, 2023, § 202a Rn. 8.
[77] *Butler/McDaniel/Farley/Rexford*, A Survey of BGP Security Issues and Solutions, Proceedings of the IEEE, Vol. 98, No. 1, 2010, 100 (100).
[78] *Fischer*, StGB, 2023, § 202b Rn. 3.

2.1.2.5 Vorbereitung einer Computerstraftat, § 202 c Abs. 1 Nr. 2 StGB

Darüber hinaus kann nach der hier vertretenen Meinung eine Strafbarkeit des IT-Sicherheitsforschenden nach § 202 c Abs. 1 Nr. 2 StGB in dem hier diskutierten Fall regelmäßig ausgeschlossen werden. Hiernach macht sich strafbar, wer eine Straftat nach § 202 a oder § 202 b StGB vorbereitet, indem er Computerprogramme *verwende*t, deren Zweck die Begehung solcher Taten ist. Selbst wenn der IT-Sicherheitsforschende für die Verbreitung der Update-Nachricht dasselbe Computerprogramm wie der Angreifer nutzt, scheitert eine Strafbarkeit nach § 202 c Abs. 1 Nr. 2 StGB bereits am mangelnden Vorsatz, denn der hier unterstellte „gutwillige Umgang" des IT-Sicherheitsforschenden mit den Softwareprogrammen soll gerade nicht von der Norm erfasst werden.[79] Der IT-Sicherheitsforschende verwendet in dem hier untersuchten Szenario regelmäßig auch keine Software, dessen funktionaler Zweck krimineller Natur ist.[80]

2.1.2.6 Computersabotage § 303 b Abs. 1 Nr. 1, 2 StGB

Eine Strafbarkeit des IT-Sicherheitsforschenden nach § 303 b Abs. 1 Nr. 1, 2 StGB könnte sich ergeben, wenn dieser eine Datenverarbeitung, die für einen anderen von wesentlicher Bedeutung ist, erheblich stört. Schutzgut des § 303b StGB ist das Interesse der Betreiber und Nutzer von Datenverarbeitungsanlagen an deren ordnungsgemäßer Funktionsweise.[81] Nach § 303 b Abs. 1 StGB ist jedoch nur die erhebliche Störung der Funktionsfähigkeit eines Computersystems strafbar. Dabei sind die Anforderungen hoch. So liegt eine erhebliche Störung des lokalen Netzwerkes nur dann vor, wenn die Internetkommunikation durch die Maßnahme gänzlich unterbunden wird.[82] Im Verteidigungsfall kommt es durch die Änderung der Routingtabellen nicht zu einer gänzlichen Unterbindung des Internetverkehrs, sodass keine schwere Störung des lokalen Netzwerks vorliegt. Der IT-Sicherheitsforschende leitet allein den an die IP-Adresse des Angegriffenen gerichteten Datenverkehr an diesen um und stört somit regelmäßig nicht die gesamte Funktionsfähigkeit eines Computersystems. Somit ist nach der hier vertretenen Meinung i.d.R. auch eine Strafbarkeit der IT-Sicherheitsforschenden nach § 303 b Abs. 1 Nr. 1, 2 StGB ausgeschlossen.

2.2 Abkoppeln oder Übernehmen von für Angriffe genutzten Netzwerk-Ressourcen

Ein weiteres Instrument der aktiven Cyberabwehr ist das Abkoppeln oder Übernehmen von für Angriffe genutzten Netzwerk-Ressourcen, namentlich IT-Infrastrukturen, die von böswilligen Angreifern zur Kontrolle und Kommunikation mit einer von ihnen verteilten Schadsoftware sowie zum Abgreifen der gestohlenen Daten gebaut werden (sog. Command-and-Control (C2-)Server).[83] Die klassischen Ziele der hier beschriebenen Cyberabwehrmaßnahme sind vorrangig das Stoppen von Distributed-Denial-of-Service

[79] BT-Drs. 16/3656, S. 18.
[80] *Wagner,* PinG 2020, 66 (70).
[81] Vgl. BT-Drs. 16/3656, S. 22.
[82] Vgl. *Hassemer,* in: Auer-Reinsdorff/Conrad, Handbuch IT- und Datenschutzrecht, 2019, Rn. 269.
[83] *Shulman/Waidner,* Athene Whitepaper, Aktive Cyberabwehr, 2022, über: https://www.athene-center.de/fileadmin/Downloads/aktive-cyberabwehr.pdf, S. 4 f.

(DDoS)-Angriffen[84] und das Unterbinden der Kommunikation zwischen einem Botnetz[85] und seiner C2-Infrastruktur.[86] Da die für Cyberangriffe genutzten Netzwerk-Ressourcen regelmäßig für eine Vielzahl von Angriffen verwendet werden, trägt ihre erfolgreiche Abschaltung wesentlich dazu bei, derzeit stattfindende Cyberangriffe reaktiv zu stoppen und künftige Bedrohungen präventiv zu verhindern.[87]

Eine Auswertung der jüngsten Cyberabwehrmaßnahmen und der hierdurch gewonnenen Erkenntnisse unterstreicht die praktische Durchführbarkeit und Effektivität dieser Methode. So ist es dem Bundeskriminalamt (BKA) und der Generalstaatsanwaltschaft Frankfurt am Main – Zentralstelle zur Bekämpfung der Internetkriminalität (ZIT) – im Mai 2024 unter Beteiligung des Bundesamts für Sicherheit in der Informationstechnik (BSI) gelungen, die technische Infrastruktur der Schadsoftware *Smokeloader* im Zuge der internationalen „*Operation Endgame*" zu beschlagnahmen, die Kontrolle über die C2-Infrastruktur der Angreifer zu übernehmen sowie ihnen den Zugriff auf tausende Opfersysteme zu entziehen.[88] Durch Umleitung der Kommunikation der Schadsoftware auf eine behördliche, so genannte Sinkholing-Infrastruktur konnten weltweit über 1.300 kriminell genutzte Internetdomänen unschädlich und über 100 Server beschlagnahmt werden. Bereits zuvor ist es internationalen Strafverfolgungs- und Justizbehörden im Januar 2021 gelungen, EMOTET, eines der professionellsten und gefährlichsten Botnetze des letzten Jahrzehnts, zu zerschlagen, indem in einer international konzertierten Aktion, u.a. von Europol und Eurojust koordiniert, die Kontrolle über die täterseitig genutzte Server-Infrastruktur übernommen und durch behördliche Sinkhole-Server ersetzt wurde.[89] Durch die von Experten anschließend durchgeführte Anpassung der Malware konnten sodann über 53.000 betroffene Systeme identifiziert und zahlreiche Server in Deutschland und weltweit beschlagnahmt werden.[90]

2.2.1 Technische Grundlagen

Ein effektiver Ansatz zur Abwehr von Angriffen durch Botnetze[91] und andere Formen von Schadsoftware ist der Einsatz sogenannter *Sinkhole-Server* (auch bekannt als *DNS-Sinkhole*) zur Abkopplung oder Übernahme täterseitig genutzter Netzwerk-Ressourcen.

---

[84] Bezeichnet eine in feindseliger Absicht herbeigeführte Überlastung oder stark eingeschränkte Verfügbarkeit von IT-Infrastrukturen und Internetdiensten (z.B. Webseiten und Server) durch Einsatz große Botnetze aus mit Schadsoftware infizierten Systemen.

[85] *Dukek*, DuD 2024, 153: „*Ein Botnetz ist ein Netzwerk von mit dem Internet verbundenen Geräten, die durch Malware infiziert und ferngesteuert werden. Diese Geräte, oft als „Bots" bezeichnet, können Computer, Server, Smartphones oder andere vernetzte Geräte sein. Sie werden häufig für bösartige Aktivitäten wie das Versenden von Spam, das Durchführen von Distributed Denial-of-Service (DDoS)-Angriffen und Ähnlichem verwendet.*"

[86] *Shulman/Waidner,* Athene Whitepaper, Aktive Cyberabwehr, 2022, über: https://www.athene-center.de/fileadmin/Downloads/aktive-cyberabwehr.pdf, S. 7 f.

[87] *Shulman/Waidner,* Athene Whitepaper, Aktive Cyberabwehr, 2022, über: https://www.athene-center.de/fileadmin/Downloads/aktive-cyberabwehr.pdf, S. 8.

[88] *BKA,* Operation „Endgame": Bundeskriminalamt und internationalen Partnern gelingt bisher größter Schlag gegen weltweite Cybercrime, über: www.bka.de/DE/DasBKA/OrganisationAufbau/Fachabteilungen/Cybercrime/Endgame/Endgame_node.html

[89] *Europol*, World's most dangerous malware EMOTET disrupted through global action, über: www.europol.europa.eu/media-press/newsroom/news/world%e2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action

[90] *Autig* in: Rüdiger/Bayerl, Hdb. Cyberkriminologie 2, Ransomware als Business Case in der organisierten Kriminalität, S. 349.

[91] *Kochheim*, Cybercrime und Strafrecht in der Informations- und Kommunikationstechnik, S. 335 Rn. 878 mit Verweis auf BR-Drs. 338/16, 2 (2016): "*Als ein Botnetz bezeichnet man eine große Anzahl von mit dem Internet ständig oder zeitweise verbundener informationstechnischer Systeme wie Computer oder Mobiltelefone, die – von ihrem rechtmäßigen Nutzer unbemerkt – mit Schadprogrammen infiltriert sind und daher einzeln oder in ihrer Gesamtheit einer fremden Kontrolle unterliegen.*"*-Programme sind Malware, die sich auf die Fernsteuerung fremder Computer (Zombies) konzentriert.*"

Die Grundidee des sogenannten Sinkholing als aktive Verteidigungsmaßnahme basiert auf dem für die Kommunikation zwischen Computer und Internet zuständige *Domain Name System* (auch als *DNS* bekannt). Das DNS ist ein weltweit auf eine Vielzahl von DNS-Servern verteilter, dezentraler wie auch hierarchisch angeordneter Verzeichnisdienst, dessen Funktion darin besteht, die für Menschen lesbaren Domainnamen (z.B. www.enisa.europa.eu) auf für den Computer ansprechbare, nummerische IP-Adressen (z.B. IPv4-Adressen wie 212.146.105.104 oder IPv6-Adressen wie 2400:cb00:2048:1::c629:d7a2) abzubilden – vergleichbar mit einer Art „Telefonbuch des Internets".[92] Versucht bspw. ein Nutzer eine Webseite durch Eingabe eines Domainnamen in die Adresszeile seines Webbrowsers aufzurufen, so wird - vereinfacht skizziert - in technischer Hinsicht zunächst eine DNS-Anfrage an den für den Nutzer zuständigen DNS-Server gestellt, der regelmäßig dem ISP (Internet Service Provider) des Nutzers zugehörig ist. Dieser nimmt sodann die Anfrage primär entgegen, gleicht diese mit den in seiner Datenbank vorgehaltenen DNS-Einträgen ab und beantwortet die Anfrage, sofern vorhanden, mit der zum Domainnamen gehörenden IP-Adresse.[93] Ist hingegen ein entsprechender DNS-Eintrag nicht in der Datenbank gespeichert, so wird die Anfrage so lange weitergeleitet, bis sie den für den Domainnamen verantwortlichen DNS-Server erreicht und dieser dann die Anfrage mit der zugehörigen IP-Adresse beantwortet.[94]

Die Methode des Sinkholing nutzt die zuvor beschriebene Funktionsweise des *DNS* und kombiniert sie mit der Expertise über die autonome Vorgehensweise des Bots, der zur Kontrollerlangung und (Fern-)Steuerung auf dem Zielgerät von den Angreifern installiert wird. Hierzu verbindet der Bot das infiltrierte Gerät mit dem Command-and-Control (C2)-Server der Angreifer unter Verwendung speziell eingerichteter Domainnamen, um sodann von diesem Instruktionen wie die zur Durchführung eines Denial-of-Service (DoS) Angriffs oder dem Versenden von Spam- oder Phishing-Nachrichten zu empfangen, weitere schädliche Dateien (Programmcode) herunterzuladen und ausgespähte Daten zu übermitteln – s. Abb. 2.[95] Die Effizienz von „Bot-Angriffen" hängt maßgeblich von den zur Verfügung stehenden Ressourcen des infizierten Geräts ab (z.B. verfügbare Bandbreite oder generierbare Pakete pro Sekunde), sodass Angreifer darauf abzielen, eine möglichst hohe Anzahl von Geräten (i.d.R. hunderte bis tausende[96]) mit Bots zu infizieren und diese zu einem sogenannten Botnetz zum Zwecke ihrer gleichzeitigen Steuerung zu gruppieren.

---

[92] *Schmidt/Pruß*, in: Auer-Reinsdorff/Conrad, IT-R-HdB, § 3 Technische Grundlagen des Internets Rn. 86; Sohr/Kemmerich, in: Kipker Cybersecurity, Kap. 3 Technische Grundlagen der Informationssicherheit, Rn. 135; *Kochheim*, Cybercrime und Strafrecht in der Informations- und Kommunikationstechnik, S. 68 Rn. 162 f.; Europäische Agentur für Cybersicherheit (ENISA), DNS-Sinkhole, über: https://www.enisa.europa.eu/topics/incident-response/glossary/dns-sinkhole

[93] *Sohr/Kemmerich*, in: Kipker Cybersecurity, Kap. 3 Technische Grundlagen der Informationssicherheit, Rn. 135; *Kochheim*, Cybercrime und Strafrecht in der Informations- und Kommunikationstechnik, S. 68 Rn. 163; *Eisele*, in: Hilgendorf/Kudlich/Valerius, Handbuch des Strafrechts, Bd. 6, 1. Auflage 2022, Computerstrafrecht, Rn. 128.

[94] *Schmidt/Pruß* in: Auer-Reinsdorff/Conrad IT-R-HdB, § 3 Technische Grundlagen, Rn. 103 ff.

[95] *BSI*, Botnetz Smokeloader unter Beteiligung des BSI zerschlagen, über: www.bsi.bund.de/DE/Service-Navi/Presse/Alle-Meldungen-News/Meldungen/Smokeloader_240530.html; *BKA*, Operation „Endgame": Bundeskriminalamt und internationalen Partnern gelingt bisher größer Schlag gegen weltweite Cybercrime, über: www.bka.de/DE/DasBKA/OrganisationAufbau/Fachabteilungen/Cybercrime/Endgame/Endgame_node.html

[96] *Holz*, Tracking and Mitigation of Malicious Remote Control Networks, 2.3 Bots and Botnets, Figure 2.2, S. 17.

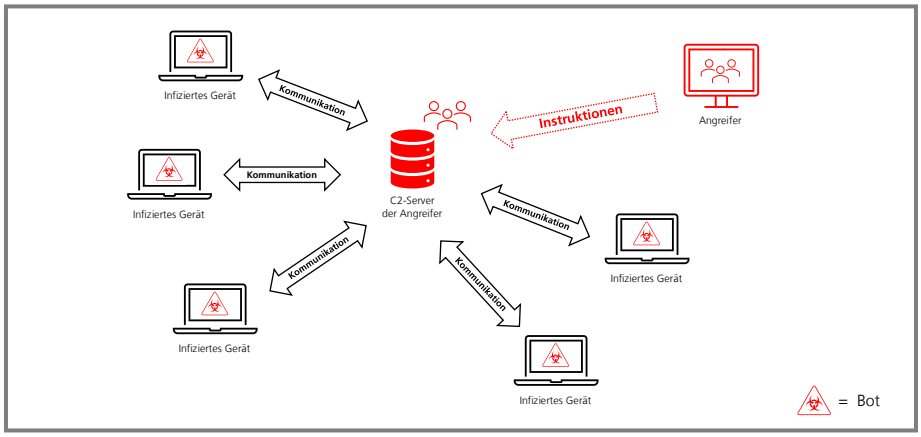

Abb. 2: Vereinfachte Darstellung eines Botnetzes mit einem zentralen C2-Server[97]

Mit dem Ziel, den vorbezeichneten Kommunikationskanal zu schließen, die missbräuchliche Fernsteuerung zu stoppen und das Botnetz durch Kontrollentzug effektiv unschädlich zu machen, setzen IT-Sicherheitsforschende und Telekommunikationsanbieter in kooperativer Zusammenarbeit sogenannte Sinkhole-Server ein. Nach Identifizierung einer verdächtigen oder bekannt maliziösen Domain nimmt der Server-Betreiber entsprechende Änderungen in den DNS-Einträgen vor, sodass DNS-Anfragen zur Angreiferdomäne, mutmaßlich von einem infizierten Gerät, abgefangen und statt der IP-Adresse des ursprünglichen Ziels (C2-Server), eine davon abweichenden IP-Adresse geliefert wird, die zu einem von Sicherheitsforschenden kontrollierten Sinkhole-Server gehört. Dieser Vorgang wird als Abkopplung bezeichnet und ist in Abb. 3 rechts zu sehen – auf der linken Seite ist der Zustand vor der Abkopplung dargestellt. Die Abkopplung ist vergleichbar mit der Änderung eines Eintrags im Telefonbuch.[98]

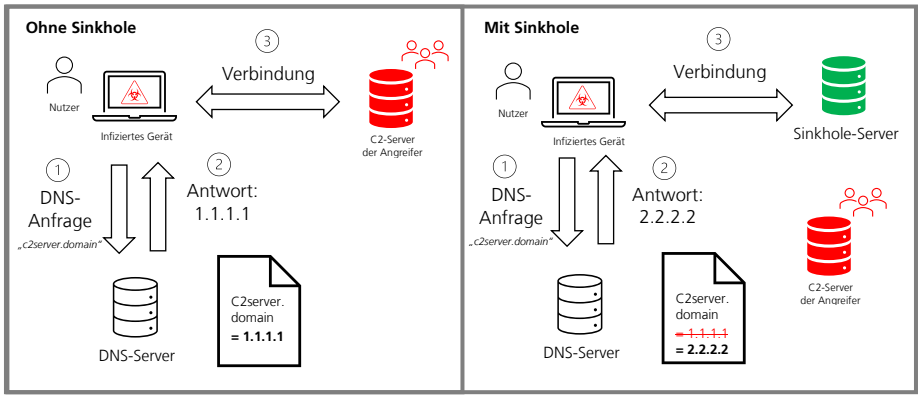

Abb. 3: Mit und ohne Umleitung an den Sinkhole durch Veränderung der DNS-Einträge[99]

Alternativ kann die Umsetzung auch mittels direkter Umleitung des IP-Datenverkehrs vom ursprünglichen Ziel (C2-Server) zum Sinkhole-Server im Wege der Zuweisung der Ziel-IP-Adresse durch die Telekommunikationsanbieter gelingen, sodass sämtlicher an diese IP-Adresse gesendeter Datenverkehr direkt an den Sinkhole-Server fließt (sog. Übernahme).[100]

---

[97] Konzept der Abbildung im Wesentlichen übernommen von: *Holz*, Tracking and Mitigation of Malicious Remote Control Networks, 4.8 Empirical Measurements, S. 58 f.
[98] *Kim/Choi/Song*, A Methodology for Multipurpose DNS Sinkhole Analyzing Double Bounce Emails, S. 610 ff.; Ritter in Kipker/Reusch/Ritter, 1. Aufl. 2023, BSIG § 7c Rn. 22 f.; *Ritter,* in Kipker/Reusch/Ritter, Recht der Informationssicherheit, 1. Aufl. 2023, BSIG § 7c Rn. 23; BT-Drs. 19/26106, 75.
[99] Konzept der Abbildung im Wesentlichen übernommen von: *ENISA, DNS-Sinkhole*, über: https://www.enisa.europa.eu/topics/incident-response/glossary/dns-sinkhole.
[100] *Ritter* in Kipker/Reusch/Ritter, Recht der Informationssicherheit, 1. Aufl. 2023, BSIG § 7c Rn. 23; BT-Drs. 19/26106, 75.

Nach erfolgreicher Durchführung der Sinkhole-Methode unter Anwendung der vorgestellten Methoden (Veränderungen von DNS-Einträgen oder Umleitung des IP-Datenverkehrs) haben die Angreifer regelmäßig keine Möglichkeit mehr, den Kontakt zwischen dem infizierten Opfersystem und dem C2-Server wiederherzustellen, sodass diese nunmehr voneinander abgekoppelt sind.

Der Sinkhole-Server überwacht und protokolliert ab diesem Zeitpunkt alle Zugriffs- und Verbdingungsversuche mit Zeitstempel, Quell-IP-Adresse sowie dem Quell-Port.[101] Eine Quell-IP-Adresse ist eine zugewiesene IP-Adresse eines Geräts, das eine Netzwerkverbindung initiiert. Sie dient zur Identifikation des Ursprungsgeräts im Netzwerk und ermöglicht es dem Empfänger von Datenpaketen, den Absender zu adressieren, um ihm zu antworten. Ein Quell-Port ist eine nummerische Kennung, die auf Senderseite Auskunft darüber gibt, welche bestimmte Anwendung auf dem Gerät, Daten über das Netzwerk verschickt. Da i.d.R. nur infizierte Geräte versuchen, sich mit dem Domainnamen zu verbinden, der auf das Sinkhole umgeleitet wird, und sich hinter diesem grundsätzlich keine legitime Internetseite befindet, indiziert ein Zugriffs- bzw. Verbindungsversuch eine Infizierung des ausführenden Geräts mit einer Schadsoftware.[102] Aufgrund der hierdurch gesammelten Informationen und der Umleitung des von Tätern ursprünglich anvisierten Datenverkehrs an das „zwischengeschaltete" Sinkhole, werden die IT-Sicherheitsforschenden in die Lage versetzt, die Daten zur Analyse und Auswertung der Schadsoftware sowie zur Identifizierung betroffener Systeme und Nutzer zu verwenden.[103]

In der Praxis findet sodann eine Benachrichtigung der für die jeweiligen IP-Adressen zuständigen Internet-Provider statt, die wiederum ggf. die betroffenen Nutzer über die Infizierung ihres Geräts informieren. Hierbei gilt zu berücksichtigen, dass die auf den betroffenen Geräten befindliche Schadsoftware trotz Abkopplung und Abschaltung der Kommunikation nicht gelöscht wird, sondern bis zur Bereinigung weiterhin auf den betroffenen Geräten existiert. Sollte es den Tätern gelingen, eine alternative Botnetz-Infrastruktur aufzubauen, kann nicht ausgeschlossen werden, dass sie zu einem späteren Zeitpunkt wieder die Kontrolle über die weiterhin vorhandenen Bots erhalten. Mithin ist eine Entfernung der Bots auf den betroffenen Geräten unabdingbar, um eine Unschädlichmachung zu gewährleisten.[104]

Ein abschließender, wenngleich kursorischer Blick auf den zu Beginn skizzierten hierarchischen Verlauf einer DNS-Anfrage zeigt, dass die Erfolgswahrscheinlichkeit der Sinkhole-Methode erheblich von der Position des Betreibers innerhalb der DNS-„Anfragekette" abhängt. Je früher der DNS-Server eines Betreibers, der sich bei dem Einsatz des Sinkhole kooperativ zeigt, vom infizierten Gerät angesprochen wird, d.h. je weiter „vorne" er in der „Anfragekette" steht, desto größer ist die Wahrscheinlichkeit, dass das Sinkholing Erfolg haben wird. Sehr große ISP wie bspw. die Deutsche Telekom

[101] *BSI*, Botnetz Smokeloader unter Beteiligung des BSI zerschlagen, über: https://www.bsi.bund.de/DE/Service-Navi/Presse/Alle-Meldungen-News/Meldungen/Smokeloader_240530.html
[102] *Ritter* in Kipker/Reusch/Ritter, Recht der Informationssicherheit, 1. Aufl. 2023, BSIG § 7c Rn. 22; Europäische Agentur für Cybersicherheit (ENISA), DNS-Sinkhole, über: https://www.enisa.europa.eu/topics/incident-response/glossary/dns-sinkhole; *BSI*, Reports zu Schadprogramm-Infektionen , über: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Reaktion/CERT-Bund/CERT-Bund-Reports/Schadprogramm-Infektionen/schadprogramm-infektionen_node.html
[103] *Ritter* in Kipker/Reusch/Ritter, Recht des Informationssicherheit, 1. Aufl. 2023, BSIG § 7c Rn. 22 f.; BT-Drs. 19/26106, 75.
[104] *BSI*, Fragen und Antworten zu Botnetzen, über: https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Botnetze/Fragen-und-Antworten/fragen-und-antworten_node.html; *Secupedia*, Gefährliches Botnetz „Smokeloader" mit BSI-Unterstützung zerschlagen, über: https://www.secupedia.de/news/gefaehrliches-botnetz-smokeloader-mit-bsi-unterstuetzung-zerschlagen/, *BSI*, Botnetz Smokeloader unter Beteiligung des BSI zerschlagen, über: https://www.bsi.bund.de/DE/Service-Navi/Presse/Alle-Meldungen-News/Meldungen/Smokeloader_240530.html

oder Vodafone zeichnen sich durch eine solche vorrangige Position aus.[105] Sollte die Zusammenarbeit mit einem solchen DNS-Betreiber nicht gelingen, so wird entweder der DNS-Server die IP-Adresse des bösartigen C2-Servers weiterhin liefern, sodass die Aktivitäten der Angreifer ohne Unterbrechung fortgesetzt werden können, oder es tritt der Fall ein, dass eine Beantwortung des vom infizierten Gerät angefragten DNS-Server mit dem Domainnamen des C2-Server mangels Zuständigkeit für diesen nicht möglich ist, sodass er die DNS-Anfrage an einen anderen DNS-Server weitergeben wird. An dieser Stelle entscheidet wiederum der kooperative Einsatz eines Sinkhole über ein Abkoppeln des infizierten Geräts vom C2-Server oder den fortgesetzten Anfrageverlauf entlang der DNS-Hierarchie.

Im Ergebnis lässt sich festhalten, dass der Erfolg der Sinkholing-Methode zunächst von der kooperativen Zusammenarbeit mit den Domain-Registrierungsstellen und DNS-Betreibern wie auch in gleichem Maße von ihrem jeweiligen DNS-Verantwortungsbereich und der Anfragewahrscheinlich ihrer DNS-Server abhängig ist. Unter Berücksichtigung der vorbezeichneten Ausführungen stellt der Einsatz von Sinkholes eine effektive Verteidigungsmaßnahme dar, um Botnets und andere bösartige Netzwerke zu erkennen, Daten über die verwendete Schadsoftware zu sammeln sowie kompromittierte Geräte zu identifizieren und diese von der Kontrolle des Täters durch Umleitung der Kommunikation abzukoppeln, um letztlich den konkreten Cyberangriff reaktiv oder präventiv unschädlich zu machen. Inwiefern sich der IT-Sicherheitsforschende unter Anwendung des Sinkholing dem Risiko eines strafrechtlich relevanten Verhaltens begibt, wird im folgenden Abschnitt bewertet.

2.2.2 Strafrechtliche Bewertung

Ein strafbares Verhalten des IT-Sicherheitsforschenden könnte in der durch die Umleitung des Datenverkehrs an einen von ihm betriebenen Sinkhole-Server und das Abfangen sowie Speichern und Analysieren der Daten des infizierten Geräts bestehen.

Von der Anwendbarkeit des deutschen Strafrechts gemäß § 3 i.V.m. § 9 Abs. 1 StGB kann vorliegend ausgegangen werden.

Erster Handlungsabschnitt: Änderung des DNS-Eintrages zum Zwecke der Umleitung an den Sinkhole-Server des IT-Sicherheitsforschenden

2.2.2.1 Datenveränderung, § 303a Abs. 1 StGB

Eine Strafbarkeit des IT-Sicherheitsforschenden aus § 303a Abs. 1 StGB scheidet bei Durchführung der vorbezeichneten Verteidigungsmaßnahme nach der hier vertretenen Meinung regelmäßig aus. Gemäß § 303a Abs. 1 StGB wird bestraft, wer rechtswidrig Daten i.S.d. § 202a Abs. 2 StGB löscht, unterdrückt, unbrauchbar macht oder verändert.

Die auf den DNS-Servern gespeicherten Informationen über die Domainnamen und die dazugehörigen IP-Adressen (sogenannte DNS-Einträge) lassen sich zunächst unter den Datenbegriff i.S.d. §§ 202 a Abs. 2, 303 a Abs. 1 StGB subsumieren. Indem nunmehr eine inhaltliche Umgestaltung der DNS-Einträge insoweit vorgenommen wird, dass die Domainnamen nunmehr auf eine andere IP-Adresse umgeleitet werden, ist auch der Tatbestand der Veränderung i.S.d § 303a Abs. 1 StGB erfüllt. Jedoch wird eine Veränderung der DNS-Einträge in der Praxis ausschließlich durch die DNS-Betreiber selbst

[105] *Wildberg/Lee-Wunderlich*, CCZ 2023, 281.

vorgenommen, sodass eine Strafbarkeit des IT-Sicherheitsforschenden nach § 303a Abs. 1 StGB in dem hier beschriebenen Fall regelmäßig nicht in Betracht kommt.

2.2.2.2 Computersabotage, § 303b Abs. 1 StGB

Eine Strafbarkeit des IT-Sicherheitsforschenden nach § 303b Abs. 1 Nr. 1 bis Nr. 3 StGB kann in dem hier diskutierten Fall nach der hier vertretenen Meinung ebenso regelmäßig ausgeschlossen werden. Hiernach macht sich strafbar, wer eine Datenverarbeitung, die für einen anderen von wesentlicher Bedeutung ist, erheblich stört. Selbst wenn die Umleitung des Datenverkehrs vom infizierten Gerät zum Sinkhole-Server des IT-Sicherheitsforschenden den hohen Anforderungen an die Erheblichkeit einer Störung genügen würde, so muss an dieser Stelle wiederum festgestellt werden, dass nicht der IT-Sicherheitsforschende die von § 303b Abs. 1 Nr. 1 bis Nr. 3 StGB sanktionierten Tathandlungen begeht, sondern die Veränderung der Einträge im DNS als Ursache der Umleitung vielmehr vom DNS-Betreiber selbst durchgeführt wird.

Zweiter Handlungsabschnitt: Empfangen sowie Speichern und Analysieren der Daten des infizierten Geräts nach erfolgter Umleitung auf den Sinkhole-Server

2.2.2.3 Ausspähen von Daten (zu Lasten des Opfers), § 202a Abs. 1 StGB

Der IT-Sicherheitsforschende könnte sich wegen des Ausspähens von Daten nach § 202a Abs. 1 StGB strafbar gemacht haben, indem er die nach der erfolgreichen Umleitung an seinen Sinkhole-Server weitergeleiteten Daten speichert und analysiert. Nach § 202 a Abs. 1 StGB wird bestraft, wer sich oder einem Dritten unbefugt Zugang zu Daten verschafft, die nicht für ihn bestimmt und gegen unberechtigten Zugang besonders gesichert sind.

2.2.2.3.1 Daten i.S.d Abs. 2

Tatobjekt des § 202a Abs. 1 StGB sind Daten i.S.d. Abs. 2, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden.[106] Nach h. M. ist hierbei von einem weit verstandenen Datenbegriff auszugehen, weshalb unter Daten i.S.d. § 202a StGB *„codierte Informationen jeder Art"* zu verstehen sind.[107] Das Speichern von Daten i.S.d. § 202a Abs. 2 StGB ist das Erfassen, Aufnehmen oder Aufbewahren von Daten auf einem Datenträger zum Zwecke ihrer weiteren Verarbeitung oder Nutzung, womit alle Formen der Verkörperung auf einem Datenträger geschützt sind.[108] Die Übermittlung von Daten i.S.d. § 202a Abs. 2 StGB ist die Weitergabe gespeicherter oder durch Datenverarbeitung gewonnener Daten an Dritte in der Weise, dass die Daten an den Dritten weitergegeben werden oder der Dritte zur Einsicht oder zum Abruf bereitgehaltene Daten einsieht oder abruft, wobei die Weitergabe elektronisch oder sonst auf technischem Weg (unkörperlich) mittels Netzwerk- oder Telekommunikationsverbindung, vornehmlich in Netzwerken wie WLANS oder im Internet, erfolgen muss.[109] Hiervon erfasst ist u.a. das praktisch bedeutsame Anzapfen von Datenübertragungsvorgängen.[110]

[106] *Graf,* in: MüKoStGB, StGB, 2021, § 202a Rn. 10.
[107] *Graf,* in: MüKoStGB, StGB, 2021, § 202a Rn. 12; *Binder,* Strafbarkeit intelligenten Ausspähens von programmrelevanten DV-Informationen, 1994, S. 41; *Lenckner/Eisele/Winkelbauer,* CR 1986, 483 (484); *Eisele,* in: Schönke/Schröder, StGB, 2019, § 202a Rn. 3.
[108] *Eisele,* in: Schönke/Schröder, StGB, 2019, § 202a Rn. 6; *Graf*, in: MüKoStGB, StGB, 2021, § 202a Rn. 20;
[109] *Graf*, in: MüKoStGB, StGB, 2021, § 202a Rn. 20; *Valerius*, in: Graf/Jäger/Wittig, StGB, 2024, § 202a Rn. 12; *Eisele,* in: Schönke/Schröder, StGB, 2019, § 202a Rn. 6
[110] BT-Drs. 10/5058, 28; *Heger*, in: Lackner/Kühl/Heger, StGB, 2023, § 202a Rn. 2.

Betrachtet man zunächst die Informationen, die mithilfe der Schadsoftware im Auftrag der Angreifer vom infizierten Gerät ursprünglich an den C2-Server gesendet werden sollen, aber nunmehr infolge der Veränderung der DNS-Einträge an den Sinkhole-Server weitergeleitet werden, so lassen sich diese unter den Datenbegriff subsumieren. Abhängig von den täterseitig verfolgten Zielen und einer entsprechenden Beauftragung der Schadsoftware sind die hierfür relevanten Informationen regelmäßig auf der Festplatte des Opfersystems gespeichert und befinden sich bei Ausführung der Schadsoftware in einem Datenübertragungsvorgang in Richtung auf den C2-Server, sodass es sich um übermittelte Daten i.S.d. § 202a Abs. 1 StGB handelt.

Darüber hinaus zeichnet der Sinkhole-Server (zum Zwecke der Beweissicherung und zur Identifizierung der Betroffenen) sämtliche Verbindungsversuche des Opfersystems mit dem C2-Server in Form von Quell-IP-Adresse und Quell-Port auf und ergänzt sie um einen Zeitstempel. Sowohl Quell-IP-Adressen als auch Quell-Ports werden typischerweise in einem für eine Datenverarbeitungsanlage erkennbarem Format codiert und nicht unmittelbar wahrnehmbar gespeichert (z.B. auf Speichermedien, Server-Logs oder Router-Protokollen) oder als wesentlicher Bestandteil einer jeden Netzwerkkommunikation übermittelt. Mithin handelt es sich auch hier um Daten i.S.d. § 202a StGB.[111]

2.2.2.3.2 Nicht für den Täter bestimmt

Weiterhin setzt das Ausspähen von Daten nach § 202a Abs. 1 StGB voraus, dass diese nicht für den Täter bestimmt sind. Hierbei handelt es sich um ein den objektiven Tatbestand ausschließendes Merkmal.[112] Maßgebend für die Bestimmung ist der Wille des Verfügungsberechtigten, d.h. desjenigen, der zum Zeitpunkt der Tat die Verfügungsmacht über die Daten inne hat.[113] Für die Frage des Entstehens der Verfügungsmacht ist dabei weder das Eigentum noch der Besitz am Datenträger oder die Tatsache, dass die Daten den Täter selbst betreffen, von Relevanz.[114] Bei gespeicherten Daten wird die Verfügungsmacht durch das erstmalige Erstellen und Abspeichern durch den sog. Skribenten begründet.[115] Bei übermittelten Daten ist Berechtigter grundsätzlich zunächst nur der Übermittler selbst, wobei dieser die Verfügungsberechtigung auf den Empfänger übertragen kann – z.B. wenn Daten für den Empfänger auf einem Server zum Abruf bereitgehalten sind und dieser von seinem Abrufsrecht Gebrauch macht.[116] In dem hier untersuchten Szenario erfolgt sowohl die ursprünglich von den Angreifern initiierte Datenübertragung an den C2-Server als auch die von dem IT-Sicherheitsforschenden eingestellte Datenweiterleitung an den Sinkhole-Server ohne Einverständnis und gegen den Willen des Berechtigten. Mithin sind die Daten nicht für den IT-Sicherheitsforschenden i.S.d. § 202a Abs. 1 StGB bestimmt.

2.2.2.3.3 Gegen unberechtigten Zugang besonders gesichert

Ferner müssten die Daten mit einer besonderen Zugangssicherung gegen einen unberechtigten Zugriff gesichert sein. Eine solche Zugangssicherung liegt vor, wenn Vorkehrungen vorhanden sind, die objektiv geeignet und subjektiv nach dem Willen des Berechtigten dazu bestimmt sind, den Zugriff auf die Daten auszuschließen oder

[111] *Eisele*, in: Schönke/Schröder, StGB, 2019, § 202a Rn. 6; *Buermeyer*, HRRS (8) 2004, S. 286.
[112] BT-Drs. 10/5058, 28; Fischer Rn. 7; LKH/Heger Rn. 3; *Graf*, in: MüKoStGB, 2021, Rn. 21.
[113] *Weidemann*, in: BeckOK StGB, 2024, § 202a Rn. 8.
[114] *Weidemann*, in: BeckOK StGB, 2024, StGB § 202a Rn. 9; *Graf,* in: MüKoStGB, 2021, § 202a StGB, Rn. 22.
[115] *Graf,* in: MüKoStGB, 2021, § 202a StGB, Rn. 21; *Eisele*, in Schönke/Schröder, StGB, 30. Aufl. .2019, StGB § 202a Rn. 9; *Weidemann*, in: BeckOK StGB, v. Heintschel-Heinegg/Kudlich, 61. Ed. 1.5.2024, StGB § 202a Rn. 9.
[116] BT-Drs. 16/3656, S.9; *Eisele*, in: Schönke/Schröder, StGB, 2019, § 202a Rn. 10; *Valerius*, in: Graf/Jäger/Wittig, 2024, StGB § 202a Rn. 15, 23.

wenigstens nicht unerheblich zu erschweren.[117] Bei im Übertragungsstadium befindlichen Daten – wie hier – kommen, solange sie „unterwegs" sind, als Sicherungsmaßnahmen im Wesentlichen nur die verschiedenen Möglichkeiten der Datenverschlüsselung in Betracht.[118] Das Abfangen der Daten durch den IT-Sicherheitsforschenden müsste somit unter Überwindung einer solchen Zugangssicherung erfolgen. Nach Änderung des DNS-Eintrages durch den DNS-Betreiber wird die ohnehin bereits durch die Schadsoftware der Angreifer initiierte und bestehende Datenübertragung vom infizierten Gerät zum C2-Server lediglich abgekoppelt und auf den Sinkhole-Server umgeleitet. Besondere Schutzeinrichtungen, die einen unberechtigten Zugang auf diese betroffenen Daten zumindest erheblich erschweren und die der IT-Sicherheitsforschende zunächst noch überwinden müsste, wie eine etwaige Datenverschlüsselung, liegen grundsätzlich nicht vor.

2.2.2.3.4 Zwischenfazit § 202a Abs. 1 StGB

Mithin mangelt es für das Bejahen einer Strafbarkeit des IT-Sicherheitsforschenden nach § 202a Abs. 1 StGB nach der hier vertretenen Meinung i.d.R. bereits an der erforderlichen Zugangssicherung der betroffenen Daten.

2.2.2.4 Abfangen von Daten, § 202b Abs. 1 StGB

Eine Strafbarkeit des IT-Sicherheitsforschenden könnte sich aus § 202b Abs. 1 StGB ergeben. Hiernach macht sich strafbar, wer unbefugt Daten abfängt. Geschützt werden nicht öffentliche Daten, die sich in einem Übermittlungsvorgang befinden.[119]

2.2.2.4.1 Nicht für den Täter bestimmte Daten i.S.d. § 202a Abs. 2 StGB

Mit Verweis auf die vorstehenden Ausführungen unter 2.1.2.3.1 und 2.1.2.3.2 handelt es sich im dem hier untersuchten Fall um Daten i.S.d. § 202 a Abs. 2 StGB, die nicht für den Täter bestimmt sind.

2.2.2.4.2 Nichtöffentliche Datenübermittlung

Das Abfangen von Daten nach § 202b Abs. 1 StGB setzt weiterhin voraus, dass diese während einer nichtöffentlichen Datenübermittlung verschafft wurden. Der Begriff der Datenübermittlung erfasst sämtliche Formen der elektronischen Datenübermittlung, insbesondere per E-Mail, Telefon, Telefax, VPN-Übermittlung, WLAN, UMTS, LTE.[120] Ferner müssen die Daten sich zum Zeitpunkt der Tat in einem Übertragungsvorgang befinden.[121] Vorliegend werden Daten, die sich ursprünglich auf dem Gerät des Opfers befanden und nunmehr zielgerichtet mithilfe einer Schadsoftware per Internet auf den C2-Server der Angreifer übertragen werden durch Umleitung des aktiven Datenverkehrs und Übertragungsvorgangs an den Sinkhole-Server der IT-Sicherheitsforschenden übermittelt. Eine Datenübermittlung i.S.d. § 202b Abs.1 StGB liegt vor.

Ferner müsste es sich um eine nichtöffentliche Datenübermittlung handeln. Fraglich ist, wie der Begriff der Nichtöffentlichkeit auszulegen ist. Nach der Intention des Gesetzgebers soll zur Auslegung auf die Grundsätze des nichtöffentlich gesprochenen Wortes nach § 201

[117] *Graf*, in: MüKoStGB, 2021, § 202a StGB, Rn. 35; *Eisele*, in: Schönke/Schröder, StGB, 2019, § 202a StGB, Rn. 14; vgl. BT-Drs. 16/3656 S. 10.
[118] *Eisele*, in: Schönke/Schröder, StGB, 2019, § 202a StGB, Rn. 16; *Graf*, in: MüKoStGB, 2021, § 202a StGB, Rn. 40 ff.
[119] *Fischer*, StGB, 2023, § 202b StGB, Rn. 3.
[120] *Valerius*, in: Graf/Jäger/Wittig, 2024, § 202b StGB, Rn. 5; BT-Drs. 16/3656, 11; *Graf*, in: MüKoStGB, 2021, § 202b Rn. 9; *Heger*, in: Lackner/Kühl/Heger, 2023, StGB, § 202b StGB, Rn. 2; *Cornelius*, in: Taeger/Pohle ComputerR-HdB, 102 Besonderer Teil des Strafgesetzbuches Rn. 42.
[121] *Valerius*, in: Graf/Jäger/Wittig, 2024, § 202b StGB, Rn. 5; *Eisele*, in: Schönke/Schröder, 2019, StGB § 202b Rn. 4.

Abs. 2 Nr. 2 StGB zurückgegriffen werden.[122] Danach ergibt sich, dass jegliche nichtöffentliche Datenübertragung, unabhängig von der Tragweite des Inhalts, vor einer Aufzeichnung bzw. der Verschaffung der übertragenen Daten geschützt ist. So kann auch eine Übermittlung über das Internet nichtöffentlich sein, selbst wenn es sich bei den übermittelten Daten um Informationen öffentlich zugänglicher Art handelt.[123] Bezugspunkt der Nichtöffentlichkeit i.S.d. § 202b Abs. 1 StGB ist nicht die Art oder der Inhalt der übermittelten Daten, sondern die Art des Übermittlungsvorgangs als solcher.[124]

Letztlich kommt es für die Frage der Nichtöffentlichkeit darauf an, ob die Datenübertragung an einen größeren, nach Zahl und Individualität unbestimmten und unüberschaubaren Adressatenkreis oder an einen durch persönliche oder sachliche Beziehungen miteinander verbundenen, abgegrenzten Personenkreis gerichtet und nur für diesen bestimmt ist.[125] Entscheidend ist die konkrete Bestimmung des Datenberechtigten[126] bzw. der Wille des Absenders[127]. Das schließt Fälle wie den Datenversand in privaten Netzwerken per WLAN oder Intranet, aber auch den klassischen Informationsaustausch per Telefon, Telefax sowie die Kommunikation über das Internet wie z.B. die Übertragung von E-Mails oder Kommunikationsdaten in Chaträumen oder über Messaging-Dienste ein.[128]

In dem hier diskutierten Fall hat der Verfügungsberechtigte bzw. Absender (hier das Opfer) von der Infizierung seines Geräts und der durch die Angreifer mithilfe der Schadsoftware gesteuerten Datenübermittlung regelmäßig keine Kenntnis. Gleiches gilt für die Umleitung des Datenverkehrs an den Sinkhole-Server der IT-Sicherheitsforschenden. Vielmehr findet die Datenübermittlung ohne jegliche Form der aktiven oder passiven Beteiligung sowie ohne willentliche Zustimmung des Opfers statt. Mithin liegt weder ein bewusstes Bestimmen noch eine willentliche Beschränkung des Empfängerkreises i.S.e. nichtöffentlichen Datenübermittlung durch das Opfer vor. Selbst unter Berücksichtigung eines etwaig vorhandenen mutmaßlichen Willens des Opfers dürfte dieser darauf gerichtet sein, weder eine Datenübermittlung an die Angreifer noch an den IT-Sicherheitsforschenden zu unternehmen. Der gegenständliche Fall ist vom Tatbestand des § 202b Abs. 1 StGB somit nicht erfasst.

2.2.2.4.8 Zwischenfazit § 202b Abs. 1 StGB

Eine Strafbarkeit des IT-Sicherheitsforschenden gem. § 202b Abs. 1 StGB wegen des Empfangens der nach erfolgreicher Umleitung an seinen Sinkhole-Server weitergeleiteten Daten ist nach der hier vertretenen Meinung regelmäßig mangels Nichtöffentlichkeit der Datenübermittlung ausgeschlossen.

2.2.2.5 Vorbereitung einer Computerstraftat, § 202c Abs. 1 Nr. 2 StGB

Ferner liegt nach der hier vertretenen Meinung keine Strafbarkeit des IT-Sicherheitsforschenden nach § 202c Abs. 1 Nr. 2 StGB vor. Hiernach macht sich strafbar, wer eine Straftat nach § 202a oder § 202b StGB vorbereitet, indem er

[122] BT-Drs. 16/3565, 11; *Kargl*, in: Kindhäuser/Neumann, 6. Aufl. 2023, § 202b StGB, Rn. 7.
[123] *Graf*, in: MüKoStGB, 4. Aufl. 2021, § 202b StGB, Rn. 10
[124] BT-Drs. 16/3656, 11; *Graf*, in: MüKoStGB, 2021, § 202b StGB, Rn. 10; Heger, in: Lackner/Kühl/Heger, 2023, StGB § 202b Rn. 2; *Valerius*, in: Graf/Jäger/Wittig, 2024, § 202b StGB, Rn. 6
[125] *Weidemann*, in: BeckOK StGB, 62. Ed. 1.8.2024, StGB § 202b StGB, Rn. 6; *Graf*, in: MüKoStGB, 2021, § 202b Rn. 10; Ernst, NJW 07, 2663.
[126] *Graf*, in: MüKoStGB, 4. Aufl. 2021, StGB § 202b Rn. 10
[127] *Weidmann*, in: BeckOK StGB, 62. Ed. 1.8.2024, StGB § 202b Rn. 6; *Eisele*, in: Schönke/Schröder/Eisele, 30. Aufl. 2019, StGB § 202b Rn. 4a; *Altenhain,* in: Matt/Renzikowski, 2. Aufl. 2020, StGB § 202b Rn. 5
[128] *Kochheim*, Cybercrime Ren. 646; *Hilgendorf*, in: LK-StGB, § 202b StGB, Rn. 9; *Weidemann*, in: BeckOK StGB, § 202a StGB, Rn. 6; *Valerius*, in: Graf/Jäger/Wittig, 3. Aufl. 2024, § 202b StGB, Rn. 6.

Computerprogramme herstellt, verschafft, verkauft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, deren Zweck die Begehung solcher Straftaten ist. Ergänzend zu den Ausführungen unter 2.1.2.5. gilt für den gegenständlichen Fall, dass die hier vom IT-Sicherheitsforschenden verwendeten Softwareprogramme gerade nicht nach Art und Weise ihres Aufbaus oder ihrer Beschaffenheit für die Nutzung zu illegalen Zwecken angelegt sind.[129] Vielmehr handelt es sich bei den verwendeten Programmen zum Betrieb des Sinkhole-Servers sowie zum Abfangen und Speichern des weitergeleiteten Datenverkehrs um solche, die erst durch eine missbräuchliche Anwendung zu einem Tatwerkzeug werden.[130] Eine bloße Eignung der Softwareprogramme zur Begehung einer Straftat nach § 202a oder § 202b StGB genügt hingegen nicht.[131] Zudem mangelt es für eine Strafbarkeit nach § 202c Abs. 1 Nr. 2 StGB bereits am Vorsatz zur Vorbereitung einer Straftat nach § 202a oder § 202b StGB, denn der hier zu unterstellende „gutwillige Umgang" des IT-Sicherheitsforschenden mit den Softwareprogrammen soll gerade nicht in den Anwendungsbereich der Norm fallen.[132]

2.3 Beseitigung von Schwachstellen und Schadsoftware auf den Systemen der Opfer

Botnets bestehen i.d.R. aus Hunderten bis Tausenden, in einigen Fällen sogar aus mehreren Hunderttausenden infizierter Geräte (sogenannte *Bots*).[133] Ein mit diesen Ressourcen ausgestatteter Cyberangriff bietet die Möglichkeit, eine Vielzahl von Opfern gleichzeitig und mit hohem Schadenspotential zu erreichen. So ist es bspw. Cyber-Kriminellen gelungen, über 1,6 Millionen[134] Geräte mit der als „König der Schadsoftware"[135] bezeichneten Malware Emotet zu infizieren und mithilfe des Emotet-Botnets einen Schaden in Höhe von mehr als 14 Millionen Euro in Deutschland und rund 2 Milliarden Euro weltweit zu verursachen.[136]

Eine Methode zur nachhaltigen Abwehr solcher Angriffe stellt die unmittelbare Beseitigung von Schwachstellen und Schadsoftware auf den bereits infizierten Geräten dar. Dabei gilt, dass mit steigender Komplexität und Größe des Botnets sich der für die Vornahme der Beseitigung erforderliche Aufwand erhöht. Angesichts der damit verbundenen praktischen Herausforderungen einer einzelfallbezogenen Umsetzung haben sich folgende Ansätze etabliert, die in der Lage sind, die Löschung der Schadsoftware und die Schließung täterseitig genutzter Schwachstellen zentral gesteuert und parallel durchzuführen:[137]

---

[129] BT-Drs. 16/3656, S. 12; *Eisele*, in: Schönke/Schröder, StGB, 2019, § 202c Rn. 4.
[130] BT-Drs. 16/3656, S. 18; *Eisele*, in: Schönke/Schröder, StGB, 2019, § 202c Rn. 4.
[131] BT-Drds. 16/3656, S. 19.
[132] BT-Drs. 16/3656, S. 18.
[133] *Netzpolitik*, Im Falle von EMOTET umfasste das Botnetz ungefähr 40.000 infizierte Systeme, über: https://netzpolitik.org/2021/emotet-darf-das-bka-schadsoftware-auf-infizierten-rechnern-manipulieren/#netzpolitik-pw; *Shulman/Waidner,* Athene Whitepaper, Aktive Cyberabwehr, 2022, über: https://www.athene-center.de/fileadmin/Downloads/aktive-cyberabwehr.pdf, S. 8.
[134] Office of Public Affairs, Emotet Disrupted in International Cyber Operation, über: https://www.justice.gov/opa/pr/emotet-botnet-disrupted-international-cyber-operation
[135] *Deutscher Bundestag*, Unterrichtung durch die Bundesregierung, Die Lage der IT-Sicherheit in Deutschland 2021, S.4, über: https://dserver.bundestag.de/btd/20/000/2000024.pdf.
[136] *Deutscher Bundestag*, Unterrichtung durch die Bundesregierung, Die Lage der IT-Sicherheit in Deutschland 2021, S. 87, https://dserver.bundestag.de/btd/20/000/2000024.pdf; *BKA*, Infrastruktur der Emotet-Schadsoftware zerschlagen, über: https://www.bka.de/DE/Presse/Listenseite_Pressemitteilungen/2021/Presse2021/210127_pmEmotet.html; *Netzpolitik*, BKA nutzt Emotet-Takedown als Türöffnung für mehr Befugnisse und neue Gesetze, über: https://netzpolitik.org/2021/schadsoftware-bereinigung-bka-nutzt-emotet-takedown-als-tueroeffner-fuer-mehr-befugnisse-und-neue-gesetze/
[137] *Shulman/Waidner,* Athene Whitepaper, Aktive Cyberabwehr, 2022, über: www.athene-center.de/fileadmin/Downloads/aktive-cyberabwehr.pdf, S. 8; *BSI*, Fragen und Antworten zu Botnetzen, über: https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-

a) Der von Sicherheitsbehörden (physisch) übernommene C2-Server der Angreifer wird eingesetzt, um die Bots zentral gesteuert abzuschalten (vgl. Beispiel „Emotet").
b) Die kooperative Zusammenarbeit mit den Herstellern von Hard- oder Software, die von einem Cyberangriff betroffen ist, wird zur Behebung missbräuchlich genutzter Schwachstellen und zur Softwarebeseitigung eingesetzt (vgl. Beispiel „Cyclops").
c) Die von den Angreifern geschaffenen Schwachstellen werden wiederum von den Sicherheitsbehörden genutzt, um den C2-Server zur Schließung der Sicherheitslücken anzuweisen (vgl. Beispiel „Hafnium").

2.3.1 Technische Grundlagen

Den Ausgangspunkt für die Beseitigung von Schwachstellen und Schadsoftware auf den Systemen der Opfer bildet regelmäßig die Identifizierung und behördliche Beschlagnahme eines für Cyberangriffe betriebenen C2-Servers, der für die Verteilung von Schadsoftware und Steuerung kompromittierter Geräte verantwortlich ist. Auf diese Weise werden IT-Sicherheitsforschende in die Lage versetzt, auf die Infrastruktur und Kommunikationskanäle der Angreifer zum Zwecke der aktiven Cyberabwehr zuzugreifen.[138] Hierauf aufbauend liefern IT-Sicherheitsforschende vom kontrollierten C2-Server – wie im Fall des Emotet-Takedown im Januar 2021 – eine angepasste Version der Schadsoftware –(„Binary")[139] aus, die das Ziel verfolgt, die ursprüngliche Schadsoftware auf einer Vielzahl betroffener Geräte unbrauchbar zu machen. Das heißt, über ein lokal, auf dem C2-Server initiiertes Update-Kommando wird eine modifizierte Version der Schadsoftware als Update auf alle mit dem C2-Server verbundenen Opfergeräte geladen. Das hierdurch (fern-)installierte Update neutralisiert sodann die Schad- und Nachladefunktion[140] der Schadsoftware, indem sie – ohne Kenntnis oder Zustimmung der Betroffenen – diese deaktiviert und anschließend in den Quarantäne-Bereich des infizierten Geräts verschoben wird. Ferner führt eine durch das Update initiierte Anpassung der Kommunikationsparameter dazu, dass die betroffenen Geräte fortan nicht mehr Kontakt mit den (übrigen) C2-Servern der Täter aufnehmen, sondern sich bei den von IT-Sicherheitsforschenden kontrollierten Sinkhole-Servern melden. Diese Server protokollieren sämtliche Verbindungsversuche mit Zeitstempel, IP-Adresse und dem von der Schadsoftware übermittelten Computernamen – Inhalte werden dabei grundsätzlich nicht ausgeleitet (vgl. Ausführungen im Kapitel unter 2.2).[141] Die Protokolldaten werden anschließend an das BSI übermittelt und an die für die IP-Adressen jeweils zuständigen Netzbetreiber bzw. Provider in Deutschland weitergeleitet, um Betroffene zu identifizieren

Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Botnetze/Fragen-und-Antworten/fragen-und-antworten_node.html; *Secupedia*, Gefährliches Botnetz „Smokeloader" mit BSI-Unterstützung zerschlagen, über: https://www.secupedia.de/news/gefaehrliches-botnetz-smokeloader-mit-bsi-unterstuetzung-zerschlagen/; *BSI*, Botnetz Smokeloader unter Beteiligung des BSI zerschlagen, über: https://www.bsi.bund.de/DE/Service-Navi/Presse/Alle-Meldungen-News/Meldungen/Smokeloader_240530.html; *Shulman/Waidner,* Athene Whitepaper, Aktive Cyberabwehr, 2022, über: www.athene-center.de/fileadmin/Downloads/aktive-cyberabwehr.pdf, S. 8.

[138] *BKA*, Infrastruktur der Emotet-Schadsoftware zerschlagen, über: www.bka.de/DE/Presse/Listenseite_Pressemitteilungen/2021/Presse2021/210127_pmEmotet.html

[139] *Deutscher Bundestag*, Unterrichtung durch die Bundesregierung, Die Lage der IT-Sicherheit in Deutschland 2021(Bundestags-Drucksache 20/24), 26.10.2021, Berlin, S. 22, über: https://dserver.bundestag.de/btd/20/000/2000024.pdf

[140] „Emotet besaß als sog. Downloader die Funktion, unbemerkt ein Opfersystem zu infizieren und weitere Schadsoftware nachzuladen, etwa zur Manipulation des Online-Bankings, zum Ausspähen von gespeicherten Passwörtern oder zur Verschlüsselung des Systems für Erpressungen", über: www.borncity.com/blog/2021/01/30/details-zur-emotet-deinstallation-durch-strafverfolger/

[141] *Deutscher Bundestag*, Unterrichtung durch die Bundesregierung, Die Lage der IT-Sicherheit in Deutschland 2021(Bundestags-Drucksache 20/24), 26.10.2021, Berlin, S. 22, über: https://dserver.bundestag.de/btd/20/000/2000024.pdf; *Bundeskriminalamt*, Infrastruktur der Emotet-Schadsoftware zerschlagen, über: www.bka.de/DE/Presse/Listenseite_Pressemitteilungen/2021/Presse2021/210127_pmEmotet.html

und über die Infektion ihrer Systeme zu benachrichtigen.[142] Letztlich führt die Lösch- bzw. Bereinigungsfunktion der installierten Update-Datei zu einer automatisierten Deinstallation der Schadsoftware auf allen infizierten Geräten und stellt durch Entfernung des Ausführungsschlüssels in der Windows-Registrierung der Geräte sicher, dass die schädlichen Module nicht mehr automatisch gestartet und alle laufenden Prozesse beendet werden.[143]

Ein vergleichbares Vorgehen zeigt sich am Fall der in den USA unternommenen Zerschlagung des Botnets Cyclops Blink[144] im Frühjahr 2022, bei der ebenfalls zunächst ein Zugang zu einem C2-Server der Angreifer sichergestellt wurde, um hiervon ausgehend Befehle an die betroffenen Opfergeräte, die aufgrund der Struktur des Botnets ihrerseits als C2-Server missbräuchlich von den Angreifern eingesetzt wurden, weiterzuleiten. In Zusammenarbeit mit den Herstellern der infizierten Geräte wurden die Geräte durch entsprechende Befehle – wiederum ohne Kenntnis oder Zustimmung der Betroffenen, aber mit US-amerikanischem Gerichtsbeschluss[145] – angewiesen, das Vorhandensein der Malware-Binärdatei zu bestätigen, die Seriennummer zu protokollieren, eine Kopie der Schadsoftware zu erstellen und die Malware-Binärdatei vom Gerät zu entfernen. Anschließend wurden Firewall-Regeln auf den Geräten der Opfer hinzugefügt, die den Fernzugriff auf die betroffene Schnittstelle blockieren sollen, sofern diese für Fernwartung aus dem Internet konfiguriert sind.[146] Nach Aussage der durchführenden Behörde habe keiner der Befehle es ihnen ermöglicht, die Inhalte oder Daten des Gerätebesitzers einzusehen oder abzurufen. Auch sei die Technik im Vorfeld getestet worden, um sicherzustellen, dass sie die Funktionalität des Geräts nicht beeinträchtigt.[147] Hinzu kommt, dass die Behörde zwar ohne Wissen oder Mitwirkung der Eigentümer der Geräte, die von den Tätern als C2-Server verwendet wurden, handelte, ein Zugriff auf die restlichen mit der Schadsoftware infizierten Geräte jedoch nicht erforderlich war. Denn bereits die Deaktivierung der C2-Server sorgte dafür, dass den Angreifern jegliche Kontrolle über die verbleibenden Geräte entzogen wurde.[148]

Eine weitere Herangehensweise zur Beseitigung von Schwachstellen und Schadsoftware auf den Systemen der Opfer stellt die durch IT-Sicherheitsforschende vorgenommene Ausnutzung der von Angreifern selbst geschaffenen Schwachstellen dar, die im Folgenden exemplarisch am Fall des sog. Hafnium-Hack dargestellt wird. Im Jahr 2021 ist es der

---

[142] *Deutscher Bundestag*, Unterrichtung durch die Bundesregierung, Die Lage der IT-Sicherheit in Deutschland 2021(Bundestags-Drucksache 20/24), 26.10.2021, Berlin, S. 22, über: https://dserver.bundestag.de/btd/20/000/2000024.pdf

[143] *Borncity.com*, Details zur Emotet Deinstallation durch Strafverfolger, über: www.borncity.com/blog/2021/01/30/details-zur-emotet-deinstallation-durch-strafverfolger/; *Silicon*, Softwareupdate löscht Emotet-Malware von infizierten PCs weltweit, über: www.silicon.de/41683949/softwareupdate-loescht-emotet-malware-von-infizierten-pcs-weltweit/amp; *Redscan*, The rise and fall of the Emotet botnet, über: www.redscan.com/news/rise-and-fall-emotet-botnet/; *Deutscher Bundestag*, Unterrichtung durch die Bundesregierung, Die Lage der IT-Sicherheit in Deutschland 2021(Bundestags-Drucksache 20/24), 26.10.2021, Berlin, S. 22, über: https://dserver.bundestag.de/btd/20/000/2000024.pdf

[144] *National Cyber Security Centre UK*, New Sandworm malware Cyclops Blink replaces VPNFilter, über: https://www.ncsc.gov.uk/news/joint-advisory-shows-new-sandworm-malware-cyclops-blink-replaces-vpnfilter#section_3

[145] *United States District Court for the Eastern District of California*, Application for s search warrant, über: https://www.justice.gov/d9/press-releases/attachments/2022/04/06/edca_sw_redacted_filed_0.pdf

[146] *CSO Deutschland*, FBI greift auf private Firewalls zu, über: https://www.csoonline.com/de/a/fbi-greift-auf-private-firewalls-zu-erneut,3673870; *Borncity*, FBI zerschlägt Cyclops Blink-Botnet der fr den russischen Geheimdienst (GRU) arbeitenden Sandworm Gruppe, über: https://www.borncity.com/blog/2022/04/07/fbi-zerschlgt-cyclops-blink-botnet-der-fr-den-russischen-geheimdiensts-gru-arbeitenden-sandworm-gruppe/

[147] *CSO Deutschland*, FBI greift auf private Firewalls zu, über: https://www.csoonline.com/de/a/fbi-greift-auf-private-firewalls-zu-erneut,3673870

[148] *Borncity*, FBI zerschlägt Cyclops Blink-Botnet der fr den russischen Geheimdienst (GRU) arbeitenden Sandworm Gruppe, über: https://www.borncity.com/blog/2022/04/07/fbi-zerschlgt-cyclops-blink-botnet-der-fr-den-russischen-geheimdiensts-gru-arbeitenden-sandworm-gruppe/

Hackergruppe Hafnium gelungen, einen Angriff auf die Microsoft Exchange-Server Struktur durchzuführen, indem sie sog. Zero-Day-Sicherheitslücken kumulativ auf Tausenden von Servern in mehr als 115 Ländern ausnutzten.[149] Während die erste Schwachstelle (CVE-2021-26855) den Angreifern ermöglichte, die reguläre Authentifizierung für den Gerätezugang zu umgehen und sich als Administrator auszugeben, dienten drei weitere Sicherheitslücken (CVE-2021-26857, CVE-2021-26858 und CVE-2021-27065) vorrangig dazu, beliebige Schadcode-Befehle auszuführen sowie Nutzerdaten abzugreifen und z.B. zur Generierung überzeugender Phishing-Mails oder zur Änderung der Mailserver-Konfiguration weiterzuverwenden.[150] Im Rahmen ihres Angriffs platzierten die Hacker sog. Web-Shells auf den Opfergeräten.[151] Hierbei handelt es sich um eine einfach zu bedienende Hacker-Software, die über eine webbasierte Schnittstelle einen dauerhaften Remote-Backdoor-Zugriff auf das infizierte System ermöglicht und die Angreifer in die Lage versetzt, jederzeit mit administrativen Rechten auf das infizierte System zuzugreifen, Kommandos und Dateien auszuführen sowie weitere Schadsoftware nachzuladen.[152] Diese Art der Hintertür ist deshalb so gefährlich, weil sie sich selbst nach Beseitigung der ursprünglichen Sicherheitslücke weiterhin auf dem Gerät befindet (sog. Persistenz[153]) und aufgrund ihrer geringen Sicherung schnell von anderen Hackern kooptiert und für andere böswillige Zwecke verwendet werden kann.[154] Spätestens mit Bekanntgabe der Schwachstellen sowie ermittelter Angriffswege veränderte sich das anfänglich noch auf ausgewählte Unternehmen konzentrierte Verhalten der Hacker zu fortan massenhaften – geradezu wahllos – und als kritisch eingestuften Angriffen gegen Tausende von Zielen und Regierungen auf der ganzen Welt.[155] Die von Microsoft veröffentlichten Sicherheitsupdates zur Schließung der Schwachstellen sowie Skripten und Erkennungstools zur Identifizierung und Beseitigung der Web-Shells führte zu einer Reduzierung der Anzahl aller verwundbaren Microsoft Exchange-Server von 40% auf etwa 22%.[156] Vor dem Hintergrund der zu diesem Zeitpunkt noch circa 13.000 weiterhin anfälligen bzw. infizierten Microsoft Exchange-Server entschieden sich die US-Behörden – namentlich das

[149] *KrebsonSecurity*, At Least 30,000 U.S. Organizations Newly Hacked Via Holes in Microsoft's Email Software, über: https://krebsonsecurity.com/2021/03/at-least-30000-u-s-organizations-newly-hacked-via-holes-in-microsofts-email-software/; *Niedersachsen Digital*, Hafnium Hack: Ablauf und FOlgen, über: https://niedersachsen.digital/hafnium-hack-ablauf-und-folgen/ ,
[150] *BSI*, Mehrere Schwachstellen in MS Exchange, über: https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2021/2021-197772-1132.pdf?__blob=publicationFile&v=8; *Verfassungsschutz Baden-Württemberg*, Microsoft Exchange: Hacker-Gruppierungen nutzen Sicherheitslücken aus, über: https://www.verfassungsschutz-bw.de/,Lde/Startseite/Meldungen+und+Archiv/Microsoft+Exchange_+Hacker-Gruppierungen+nutzen+Sicherheitsluecken+aus
[151] *BSI*, Microsoft Exchange Schwachstellen, Detektion und Reaktion, S.8 f., https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Vorfaelle/Exchange-Schwachstellen-2021/MSExchange_Schwachstelle_Detektion_Reaktion.pdf?__blob=publicationFile&v=3
[152] *BSI*, Mehrere Schwachstellen in MS Exchange, über: https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2021/2021-197772-1132.pdf?__blob=publicationFile&v=21; *U.S. Department of Justice, Office of Public Affairs*, Justice Department Announces Court-Authorized Effort to Disrupt Exploitation of Microsoft Exchange Server Vulnerabilities, über: https://www.justice.gov/opa/pr/justice-department-announces-court-authorized-effort-disrupt-exploitation-microsoft-exchange; *Niedersachsen Digital*, Hafnium Hack: Ablauf und Folgen, über: https://niedersachsen.digital/hafnium-hack-ablauf-und-folgen/
[153] *BSI*, Mehrere Schwachstellen in MS Exchange, S.2, über: www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2021/2021-197772-1132.pdf?__blob=publicationFile&v=4
[154] *Niedersachsen Digital*, Hafnium Hack: Ablauf und Folgen, über: https://niedersachsen.digital/hafnium-hack-ablauf-und-folgen/
[155] *Bundesamt für Sicherheit in der Informationstechnik*, Microsoft Exchange Schwachstellen, Detektion und Reaktion, über https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Vorfaelle/Exchange-Schwachstellen-2021/MSExchange_Schwachstelle_Detektion_Reaktion.pdf?__blob=publicationFile&v=3; *Krebs on Security*, At Least 30,000 U.S. Organizations Newly Hacked Via Holes in Microsoft's Email Software, über: https://krebsonsecurity.com/2021/03/at-least-30000-u-s-organizations-newly-hacked-via-holes-in-microsofts-email-software/; *Niedersachsen Digital*, Hafnium Hack: Ablauf und Folgen, über: https://niedersachsen.digital/hafnium-hack-ablauf-und-folgen/ ,
[156] GUTcert, Bleibt Microsoft Exchange ein beliebtes Ziel von Hackern?, über: https://www.gut-cert.de/de/news-reader/news-2021-09-bleibt-microsoft-exchange-ein-beliebtes-ziel-von-hackern

FBI –, mit richterlichem Durchsuchungs- und Beschlagnahmebeschlüssen gegen die Betreiber der Server der verbleibenden Web-Shells vorzugehen.

Im Rahmen der Durchsuchung griff das FBI unter Verwendung der von den Angreifern festgelegten Passwörter auf die installierten Web-Shells zurück und nutzte die hierdurch geschaffenen „Hintertüren" ihrerseits aus, um in die betroffenen Systeme einzudringen – ohne Mitwirkung oder Zustimmung der Betroffenen. Nach Durchführung der Beweissicherungsmaßnahmen sendete das FBI sodann über die Web-Shells selbst einen Befehl an den Exchange-Server zur Löschung der wiederum anhand ihres eindeutigen Dateipfads und -namens identifizierbaren Web-Shells – zu verstehen als ein Befehl zur Selbstlöschung (s. Abb. 4).[157] Eine über die Entfernung hinausgehende Maßnahme in Form einer Beseitigung von Schwachstellen oder zur Durchsuchung des Servers nach weiteren Schadprogrammen, die möglicherweise durch Ausnutzung der Web-Shells installiert wurden, führte das FBI nach eigenen Angaben nicht durch.[158] Ebenso sei ein Zugriff auf den Inhalte von privaten Exchange-Servern nicht erfolgt.

URL einer identifizierten Web-Shell eines Exchange-Servers:

https://webmail.[domain][.]net/aspnet_client/system_web/[FILENAME].aspx

Befehl an die Web-Shell des Exchange-Servers zur Löschung der Web-Shell:

del /f C:\inetpub\wwwroot\aspnet_client\system_web[FILENAME].aspx ⇨

https://webmail.[domain][.]net/aspnet_client/system_web/[FILENAME].aspx

Abb. 4: Exemplarischer Dateipfad und Löschbefehl[159]

2.3.2 Strafrechtliche Bewertung

Ein strafbares Verhalten des IT-Sicherheitsforschenden könnte in der Beseitigung der Schadsoftware zu Gunsten des Opfers durch das ferninstallierte Update oder durch Zugriff auf das Opfersystem und Initiierung eines Löschbefehls bestehen. Von der Anwendbarkeit des deutschen Strafrechts gem. § 3 i.V.m. § 9 Abs. 1 StGB kann vorliegend ausgegangen werden.

---

[157] *United States District Court Southern District Of Texas Houston Division*, Motion to partially unseal search warrant, über: https://content.govdelivery.com/attachments/USDOJOPA/2021/04/13/file_attachments/1753980/AUSA%20McIntyre%20Motion%20to%20Partially%20Unseal%20Search%20Warrant.pdf; *Silicon*, FBI löscht Web Shells von kompromittierten Exchange-Servern – ohne Wissen der Eigentümer, über: www.silicon.de/41683742/fbi-loescht-web-shells-von-kompromittierten-exchange-servern-ohne-wissen-der-eigentuemer; *Inside IT*, NSA und FBI helfen Microsoft mit der Exchange-Security, über: www.inside-it.ch/post/nsa-und-fbi-helfen-microsoft-mit-der-exchange-security-20210414; *Southern District of Texas, United States Attorney's Office*, Justice Department announces court-authorized effort to disrupt exploitation of Microsoft Exchange Server vulnerabilities, über: www.justice.gov/usao-sdtx/pr/justice-department-announces-court-authorized-effort-disrupt-exploitation-microsoft.

[158] *Southern District of Texas, United States Attorney's Office*, Justice Department announces court-authorized effort to disrupt exploitation of Microsoft Exchange Server vulnerabilities, über: www.justice.gov/usao-sdtx/pr/justice-department-announces-court-authorized-effort-disrupt-exploitation-microsoft; *United States District Court Southern District of Texas Houston Division*, Motion to partially unseal search warrant and related documents and proposed order, über: https://content.govdelivery.com/attachments/USDOJOPA/2021/04/13/file_attachments/1753980/AUSA%20McIntyre%20Motion%20to%20Partially%20Unseal%20Search%20Warrant.pdf

[159] Konzept der Abbildung im Wesentlichen übernommen von: *United States District Court Southern District of Texas Houston Division*, Motion to partially unseal search warrant and related documents and proposed order, S. 5, über: https://content.govdelivery.com/attachments/USDOJOPA/2021/04/13/file_attachments/1753980/AUSA%20McIntyre%20Motion%20to%20Partially%20Unseal%20Search%20Warrant.pdf .

2.3.2.1 Datenveränderung, § 303a Abs. 1 StGB

Eine Strafbarkeit des IT-Sicherheitsforschenden könnte sich zunächst aus § 303a Abs. 1 StGB ergeben. Hiernach macht sich strafbar, wer rechtswidrig Daten i.S.d. § 202a Abs. 2 StGB löscht, unterdrückt, unbrauchbar macht oder verändert.

2.3.2.1.1 Tatobjekt: Gespeicherte Daten i.S.d. § 202a StGB

Tatobjekt des § 303a Abs. 1 StGB sind *Daten* i.S.d. § 202a Abs. 2 StGB. Daten sind i.S.d. § 202a Abs. 1 StGB *gespeichert*, wenn sie zum Zweck ihrer weiteren Verwendung erfasst, aufgenommen oder aufbewahrt sind, womit alle Formen der Verkörperung auf einem Datenträger geschützt sind.[160] Die Informationen über die von den Angreifern zur Infizierung des Geräts verwendete Schadsoftware, die durch das Update-Kommando des IT-Sicherheitsforschenden geändert werden, lassen sich unter den Datenbegriff des § 202a Abs. 2 StGB subsumieren. Diese sind auf den infizierten Geräten gespeichert, sodass es sich bei den Daten der Schadsoftware in der Konsequenz um gespeicherte Daten i.S.d. §§ 202a Abs. 2, 303a Abs. 1 StGB handelt.

2.3.2.2.2 Tathandlung

Eine Strafbarkeit nach § 303a Abs. 1 StGB setzt als Tathandlung eine Umgestaltung bestehender Datenbestände voraus. Nach dem Wortlaut der Norm müsste es sich dabei um eine Löschung, Unterdrückung, Unbrauchbarmachung oder Veränderung von Daten handeln. In dem vorbezeichneten Fall kommt als Tathandlung die *Veränderung von Daten* in Betracht, worunter jede mögliche Form des inhaltlichen Umgestaltens gespeicherter Daten fällt, die eine Bedeutungsveränderung der Daten in ihrem Informationsgehalt oder Aussagewert und somit eine Funktionsbeeinträchtigung zur Folge hat.[161] Nachdem der IT-Sicherheitsforschende den C2-Server unter seine Kontrolle gebracht hat, initiiert er – ausgehend vom C2-Server oder infizierten Gerät – ein Befehl zur Durchführung eines reinigenden Updates bzw. zur direkten Löschung der Schadsoftware. Je nach Umfang und Ausgestaltung des Befehls wird die Schadsoftware auf dem Gerät gelöscht und damit der bestehende Datenbestand zu Gunsten des Angegriffen verändert. Die vom Tatbestand der Norm geforderte Tathandlung ist somit erfüllt.

2.3.2.2.3 Fremdheit der Daten

Ferner müsste es sich um fremde Daten i.S.d. § 303a Abs. 1 StGB handeln. Unter Bezugnahme der Ausführungen unter 2.1.2.2.3 setzt der Tatbestand nach h. M. dabei den Eingriff in fremde Datenverfügungsbefugnisse voraus. Unabhängig davon, ob man der Ansicht der Literatur[162] folgt, die auf das Kriterium der sachenrechtlichen Zuordnung an dem gegenständlichen Datenträger abstellt, oder der Ansicht der Rechtsprechung[163], die dem Erstskribenten, der die „Erschaffung" und erstmalige Speicherung der Daten initiiert, die Verfügungsbefugnis zuspricht, steht dem IT-Sicherheitsforschenden regelmäßig keine Befugnis zur Verfügung über die auf dem Gerät des Opfers befindlichen Daten der Schadsoftware zu, sodass diese für ihn fremd i.S.d. § 303a Abs. 1 StGB sind.

[160] *Eisele,* in: Schönke/Schröder, StGB, 2019, § 202a Rn. 14.

[161] *Hecker,* in: Schönke/Schröder, StGB, 2019, § 303a Rn. 8.
[162] *Fischer*, StGB, 2023, § 303a Rn. 5; *Heger,* in: Lackner/Kühl, StGB, 2023, § 303a Rn. 4*; Hoyer,* in: SK-StGB, StGB, 2023, § 303a Rn. 5.
[163] *Fischer,* StGB, 2023, § 303a Rn. 4a.

2.3.2.2.4 Rechtswidrigkeit als Tatbestandsmerkmal

Fraglich ist, ob das Verhalten des IT-Sicherheitsforschenden als *sozialadäquat* gewertet werden kann (vgl. Ausführungen unter 2.1.2.2.4). Das würde voraussetzen, dass das vorbezeichnete Vorgehen des IT-Sicherheitsforschenden zwar äußerlich den Tatbestand erfüllt, jedoch kein tatbestandsmäßiges Unrecht vorliegt und folglich eine Strafbarkeit nach § 303a StGB ausgeschlossen wäre.[164] Der Gedanke der Sozialadäquanz wurde für Fälle entwickelt, in denen sich eine tatbestandsmäßige Handlung im Rahmen der Rechtsordnung hält.[165] Von einer Sozialadäquanz wäre vorliegend auszugehen, wenn das oben beschriebene Vorgehen des IT-Sicherheitsforschenden ohne Beanstandung üblich geworden ist.[166]

Von einer solchen Üblichkeit kann im vorliegenden Fall der Beseitigung von Schwachstellen und Schadsoftware auf den Systemen der Opfer jedoch nicht die Rede sein, so legen die meisten IT-Sicherheitsforschenden ihre Vorgehensweisen zumeist erst gar nicht offen, wenn diese mit Strafbarkeits- und Haftungsrisiken verbunden sind, sodass von „Üblichsein" nicht die Rede sein kann.[167] Darüber hinaus scheint es schwer zu bestimmen, welche Formen des Systemzugriffs durch IT-Sicherheitsforschende als von der Allgemeinheit gebilligt und folglich im Rahmen der sozialen Handlungsfreiheit liegend, anzusehen sind. Zwar kommt IT-Sicherheitsforschenden bei der Gewährleistung der IT-Sicherheit eine unsagbar wichtige Rolle zu, dies allein kann es jedoch nicht rechtfertigen, dass IT-Sicherheitsforschenden das Recht zukommt, sich (stets straffrei) Zugang zu fremden IT-Systemen zu verschaffen. Vielmehr könnte es die Gefahr mit sich bringen, dass Forschungsinteressen als Vorwand missbraucht würden, um in fremde IT-Systeme einzudringen und Daten zweckentfremdet zu verarbeiten.[168]

Rechtswidrig ist das Verändern der Daten jedoch nur dann, wenn es ohne oder gegen den Willen des Verfügungsberechtigten vorgenommen wurde.[169] Folglich kann das *Einverständnis* des „Berechtigten" den Tatbestand des § 303a StGB ausschließen.[170] Eine Strafbarkeit des IT-Sicherheitsforschenden kann daher vermieden werden, wenn der an den Daten Verfügungsberechtigte *vor* dem Stattfinden der Verteidigungsmaßnahme sein (tatbestandsausschließendes) Einverständnis erklärt, indem er der Löschung der Schadsoftware zustimmt. Rechtsunsicherheiten entstehen hier wiederum durch die Frage, wer der „Berechtigte" ist, dessen Einverständnis einzuholen ist. Der schon oben dargestellte Streit führt auch an diesem Punkt zu einer großen Unsicherheit in der Praxis, denn um eine Strafbarkeit von IT-Sicherheitsforschenden zu vermeiden, muss die Datenverfügungsbefugnis *eindeutig* festgestellt werden. Aufgrund der Komplexität von IT-Systemen und damit einhergehend der Verhältnisse der Berechtigung an diesen Systemen ist es teilweise nur mit großem Aufwand möglich, rechtssicher festzustellen, wer die Datenverfügungsbefugnis innehat. Demgegenüber ist dieser große organisatorische Aufwand jedoch für sich genommen noch kein Grund, ohne Einverständnis auf fremde IT-Systeme einzugreifen.[171] Es empfiehlt sich deshalb, das Einverständnis des Angegriffenen einzuholen, um eine Strafbarkeit des IT-Sicherheitsforschenden bestmöglich zu

[164] Nach der h. M. und der Rspr. führt ein sozialadäquates Verhalten zu einen Tatbestandausschluss, vgl.: *Hirsch,* ZStW 74, (78); *Roxin,* in: FS Klug, 1983, S. 303; *Küpper,* GA 1987, 388; *Hassemer,* wistra 1995, 46 (81); OLG München NJW 1966, 2406; NStZ 1985, 550; BGHSt 19, 154.
[165] *Fischer*, StGB, 2023, vor § 32 Rn. 12.
[166] Vgl. zur Üblichkeit: OLG Karlsruhe, Urt. v. 26.10.1979 - 10 U 272/78.
[167] *Wagner*, PinG 2020, 66 (69).
[168] *Golla,* JZ 2021, 985 (987).
[169] *Borges/Schwenk/Stuckenberg/Wegener,* Identitätsdiebstahl und Identitätsmissbrauch im Internet, 2011, S. 234.
[170] *Wieck-Noodt,* in: MüKoStGB, StGB, 2022, § 303a Rn. 17; *Fischer*, StGB, 2023, § 303a Rn. 8.
[171] *Golla*, JZ 2021, 985 (987).

verhindern.[172] Notwendig ist eine engen Zusammenarbeit zwischen IT-Sicherheitsforschenden und dem Angegriffenen, welche mit der Verteidigungshandlung jedoch regelmäßig einverstanden sein werden, da mit der Bereinigung des infizierten Geräts die Schadsoftware entfernt und die täterseitige Kontrolle gestoppt wird. In der Praxis steht dem jedoch die Eilbedürftigkeit bei der Abwendung eines Cyberangriffs entgegen.

2.3.2.2.5 Subjektiver Tatbestand

Eine Strafbarkeit des IT-Sicherheitsforschende nach § 303a StGB setzt voraus, dass dieser bezüglich der Verwirklichung des objektiven Tatbestandes zumindest bedingt vorsätzlich gehandelt hat. Bedingt vorsätzlich handelt, wer die Tatbestandsverwirklichung für möglich hält (kognitives Element) und den Eintritt des Erfolgs billigend in Kauf nimmt (voluntatives Element).[173] Ein vorsätzliches Handeln des IT-Sicherheitsforschenden ist in dem hier diskutierten Fall regelmäßig anzunehmen, denn dieser handelt mit dem notwendigen Wissen und der Intention, dass durch sein Verhalten Daten auf den Geräten der Opfer verändert werden, die ihm nicht zur Verfügung stehen. Mithin ist ein vorsätzliches Handeln zu bejahen.

2.3.2.2.6 Rechtswidrigkeit

Das Vorgehen des IT-Sicherheitsforschenden müsste rechtswidrig sein, d.h. hierdurch müsste ein fremdes Recht verletzt worden sein. Das ist dann der Fall, wenn die Ferninstallation des Updates und Löschung der Schadsoftware auf dem infizierten Gerät ohne oder gegen den Willen des Nutzungs- oder Verfügungsberechtigten (hier das Opfer) vorgenommen wurde.[174] Eine ausdrückliche Einwilligung des betroffenen Opfers liegt i.d.R. nicht vor. In Betracht kommt somit eine *mutmaßliche Einwilligung*.[175] Grundsätzlich ist davon auszugehen, dass es dem mutmaßlichen Willen des Verfügungsbefugten entspricht, einen Eingriff in sein Gerät hinzunehmen, wenn hierdurch eine darauf befindliche Schadsoftware entfernt und ein potenzieller Schaden für ihn abgewendet werden kann. So führt im hiesigen Fall die Löschung der Schadsoftware durch das vom IT-Sicherheitsforschenden initiierte Update zu einer Unterbrechung der Kommunikation zwischen Angreifer und Opfergerät. Hierdurch wird den Angreifern sowohl die Kontrolle über das infizierte Gerät entzogen als auch eine fortgesetzte Datenübertragung, bspw. zum Zweck eines Identitätsdiebstahls oder des Diebstahls vertraulicher Dokumente, verhindert.

Zu beachten ist allerdings, dass nach dem Subsidiaritätsprinzip eine mutmaßliche Einwilligung nur dann Anwendung findet, sofern eine ausdrückliche Erklärung des Berechtigten wegen unüberwindbarer oder nur mit unverhältnismäßigen Mitteln zu überwindender Hindernisse nicht rechtzeitig eingeholt werden kann.[176]

Im vorbezeichneten Fall, in dem regelmäßig eine nicht nur unerhebliche Geräteanzahl von der beabsichtigten Bereinigung durch die IT-Sicherheitsforschenden betroffen ist, ist rein faktisch betrachtet das Einholen einer Einwilligung aller Betroffenen zwar möglich, stellt allerdings organisatorisch sowohl hinsichtlich des damit verbundenen Aufwands als auch der dafür benötigten Zeit eine beachtliche Hürde dar. Wie bereits unter 2.1.2.2.4 erörtert, ist es für Maßnahmen der aktiven Cyberabwehr und angesichts der vorliegenden

[172] Auch wenn das tatbestandsausschließende Einverständnis schon bei innerer Zustimmung des Opfers wirksam ist und eine Zustimmungserklärung somit grundsätzlich entbehrlich wäre, vgl. dazu: *Schlehofer* in MüKoStGB, StGB, 2020, vor § 32 Rn. 177.
[173] *Fischer,* StGB, 2023, § 15 Rn. 11 f.
[174] *Wieck-Noodt*, in: MüKoStGB, § 303a StGB, Rn. 17.
[175] Das Merkmal der Rechtswidrigkeit i.R.d. § 303 a StGB ist in seiner Bedeutung umstritten, folgt man der Ansicht, dass es sich bei diesem, wie bei § 303 StGB um ein allg. Deliktsmerkmal handelt, kommt daneben auch die mutmaßliche Einwilligung als Rechtfertigungsgrund in Betracht, vgl. *Fischer,* StGB, 2023, § 303a Rn. 13; *Hecker,* in: Schönke/Schröder, StGB, 2019, § 303a Rn. 10.
[176] Zum Subsidiaritätsprinzip: *Schlehofer,* in: MüKoStGB, StGB, 2020, vor § 32 Rn. 205.

Gefahrensituation dringend erforderlich, dass entsprechende Maßnahmen schnellstmöglich durchgeführt werden, um schwerwiegende Auswirkungen der Angriffe zu verhindern bzw. schnellstmöglich zu stoppen. Das vorherige Einholen einer ausdrücklichen Erklärung des Berechtigten würde dem Sinn und Zweck der praktischen Dringlichkeit erheblich widersprechen. Mithin sollte die mutmaßliche Einwilligung des Verfügungsbefugten in dem hier vorliegenden Szenario angenommen werden können, wodurch eine Strafbarkeit des IT-Sicherheitsforschenden gem. § 303a StGB entfallen würde.

Weiterhin könnte das Handeln durch einen rechtfertigenden Notstand gem. § 34 StGB den Tatbestand des § 303a Abs. 1 StGB ausschließen.[177] Die hierfür zunächst vorausgesetzte gegenwärtige und nicht anders abwendbare Gefahr für das vorrangige Rechtsgut der informationellen Selbstbestimmung sowie das Recht auf Integrität und Vertraulichkeit informationstechnischer Systeme besteht in der Infizierung des Geräts mit einer Schadsoftware, die den Angreifern die Kontrolle über das Gerät ermöglicht und sie in die Lage versetzt, sämtliche Daten des Angegriffenen auf den täterseitig genutzten C2-Server zu übertragen.[178] Ziel der Verteidigungsmaßnahme ist es, die Daten vor einem unberechtigten Zugriff zu schützen und die Funktionsfähigkeit des Opfergeräts durch Löschung der Schadsoftware wiederherzustellen. Die konkret ergriffene Maßnahme müsste zudem erforderlich, d. h. geeignet und das relativ mildeste Mittel sein. Dabei stellt die konkrete Maßnahme das relativ mildeste Mittel dar, wenn kein gleich geeignetes, aber weniger eingriffsintensives Vorgehen existiert.[179] Angesichts der bereits oben dargelegten Dringlichkeit der Maßnahme und der akuten Gefahrensituation, in der sich das Opfer bereits zu diesem Zeitpunkt befindet, scheint das Verweisen auf ein zunächst vorzunehmendes Hilfeersuchen gegenüber staatlichen Stellen zwar ein milderes, allerdings nicht gleich geeignetes Mittel zu sein. Das Gerät des Opfers, das mit der Schadsoftware infiziert wurde, empfängt regelmäßig nicht nur bereits Befehle der Angreifer, um das Gerät als Teil ihres Botnets einzusetzen, sondern überträgt im Zweifel bereits Dateien wie persönliche Informationen oder Dokumente des Opfers an die Angreifer. Ein verzögertes Einschreiten aufgrund des Wartens staatlicher Hilfsmaßnahmen kann die Wahrscheinlichkeit eines Schadenseintritts oder einer Vergrößerung des Schadens nicht nur unerheblich erhöhen. Die hier vorgenommene Verteidigungshandlung der IT-Sicherheitsforschenden wäre somit regelmäßig gerechtfertigt, sodass eine Strafbarkeit des IT-Sicherheitsforschenden auch hierdurch ausscheiden könnte.

2.1.2.2.7 Zwischenfazit § 303a StGB

Während eine Strafbarkeit des IT-Sicherheitsforschenden gem. § 303a Abs. 1 StGB nach der hier vertretenen Meinung grundsätzlich bereits durch das Einholen eines Einverständnisses bzw. über das Institut der mutmaßlichen Einwilligung des Verfügungsbefugten verhindert werden kann, ergibt sich ein den Tatbestand ausschließender Rechtfertigungsgrund nach der hier vertretenen Meinung spätestens über den rechtfertigenden Notstand gemäß § 34 StGB. Darüber hinaus würde eine Straftat nur dann verfolgt werden, wenn durch den Verfügungsbefugten ein Strafantrag gem. § 303c StGB gestellt wurde.

[177] Eine Rechtfertigung über die Notwehr, § 32 StGB scheidet aus, da die Verteidigungsmaßnahme hier gerade nicht gegenüber dem Angreifer (durch einen Eingriff in seine Server) erfolgt, sondern gegenüber einen „unbeteiligten Dritten". Die Verteidigungshandlung i.R.d. § 32 StGB darf sich grundsätzlich nur gegen den Angreifer selbst und dessen Rechtsgüter, nicht aber gegen Rechtsgüter unbeteiligter Dritter oder gar der Allgemeinheit richten, vgl. BGHSt 5, 245 (245 ff.).
[178] OLG Düsseldorf, Beschl. v. 15.10.1993, Rn. 5 ff.; *Ronellenfitsch,* DuD 2008, 110 (111).
[179] *Fischer*, StGB, 2023, § 34 Rn. 10; *Perron,* in: Schönke/Schröder, StGB, 2019, § 34 Rn. 18 ff.

2.3.2.3 Computersabotage, § 303b Abs. 1 StGB

Eine Strafbarkeit des IT-Sicherheitsforschenden nach § 303b Abs. 1 Nr. 1, 2 StGB könnte sich ergeben, wenn dieser eine Datenverarbeitung, die für einen anderen von wesentlicher Bedeutung ist, erheblich stört. Schutzgut des § 303b StGB ist das Interesse der Betreiber und Nutzer von Datenverarbeitungsanlagen an deren ordnungsgemäßer Funktionsweise.[180] Nach § 303b Abs. 1 StGB ist jedoch nur die erhebliche Störung der Funktionsfähigkeit eines Computersystems strafbar. Dabei sind die Anforderungen hoch. So liegt eine erhebliche Störung des lokalen Netzwerkes nur dann vor, wenn die Internetkommunikation durch die Maßnahme gänzlich unterbunden wird.[181]

Im Fall der Installation eines Updates und anschließender Löschung der auf dem Gerät des Opfers befindlichen Schadsoftware kommt es i.d.R. zu keiner erheblichen Unterbindung der geräteseitigen Funktionsweise, sodass keine schwere Störung i.S.d. § 303b Abs. 1 StGB vorliegt. Der IT-Sicherheitsforschende leitet durch das Update einen Vorgang ein, dessen ausschließliches Ziel die Beseitigung der Schadsoftware und Wiederherstellung der ordnungsgemäßen Funktionsweise des infizierten Geräts ist und stört somit regelmäßig nicht die Funktionsfähigkeit eines Computersystems. Somit ist nach der hier vertretenen Meinung i.d.R. auch eine Strafbarkeit der IT-Sicherheitsforschenden nach § 303b Abs. 1 Nr. 1, 2 StGB ausgeschlossen.

2.3.2.4 Ausspähen von Daten (zu Lasten des Opfers), § 202a Abs. 1 StGB

Eine Strafbarkeit des IT-Sicherheitsforschenden wegen des Ausspähens von Daten nach § 202a Abs. 1 StGB scheidet in dem hier beschriebenen Fall regelmäßig aus. Im Wege der restriktiven Auslegung und Einschränkung des Tatbestands erfasst der § 202a Abs. 1 StGB nur solche Daten, die nicht für den Täter bestimmt und gegen unberechtigten Zugang besonders gesichert sind.[182] Für eine Strafbarkeit des IT-Sicherheitsforschenden müssten somit die auf dem Gerät des Angegriffenen befindlichen sowie die vom Sinkhole-Server empfangenen Daten gegen unberechtigten Zugang besonders gesichert sein. Eine solche Zugangssicherung liegt vor, wenn Vorkehrungen vorhanden sind, die objektiv geeignet und subjektiv nach dem Willen des Berechtigten dazu bestimmt sind, den Zugriff auf die Daten auszuschließen oder wenigstens nicht unerheblich zu erschweren.[183]

Die gegenständlichen Daten sind jedoch regelmäßig weder durch Passwörter, Hardware-Sicherungen noch durch sonstige Verfahren gesichert. Etwaige bereits durch die Angreifer zuvor überwundenen und anschließend nicht mehr bestehenden Hindernisse, die keine Auswirkungen auf den Zugriff des IT-Sicherheitsforschenden haben, sind für diesen rechtlich unbeachtlich. Mithin ist nach der hier vertretenen Meinung eine Strafbarkeit des IT-Sicherheitsforschenden nach § 202a Abs. 1 StGB i.d.R. mangels Vorliegens einer Zugangssicherung ausgeschlossen.

2.3.2.5 Abfangen von Daten, § 202b Abs. 1 StGB

Eine Strafbarkeit des IT-Sicherheitsforschenden nach § 202b Abs. 1 StGB kann in dem hier diskutierten Fall regelmäßig ausgeschlossen werden. Nach § 202b Abs. 1 StGB macht sich strafbar, wer unbefugt Daten, die sich in einem nichtöffentlichen Übermittlungsvorgang befinden, abfängt.[184] Bei der Installation des Updates bzw. bei der Ausführung des Löschbefehls handelt es sich gerade nicht um das Abfangen eines fließenden

[180] Vgl. BT-Drs. 16/3656, S. 22.
[181] Vgl. *Hassemer,* in: Auer-Reinsdorff/Conrad, Handbuch IT- und Datenschutzrecht, 2019, Rn. 269.
[182] BT-Drs. 16/3656, S. 10.
[183] *Graf*, in: MüKoStGB, 2021, § 202a StGB, Rn. 35; *Eisele*, in: Schönke/Schröder, StGB, 2019, § 202a StGB, Rn. 14; vgl. BT-Drs. 16/3656 S. 10.
[184] *Fischer*, StGB, 2023, § 202b Rn. 3.

Datenverkehrs, sondern um eine Veränderung des auf den infizierten Geräten bestehenden Datenbestandes. Hinsichtlich einer etwaig durch das Update der IT-Sicherheitsforschenden verursachten Anpassung der Kommunikationsparameter, die dazu führen, dass das infizierte Gerät nicht mehr mit dem täterseitigen C2-Server kommuniziert, sondern sich bei den von den IT-Sicherheitsforschenden kontrollierten Sinkhole-Server meldet, gelten die Ausführungen unter 2.2.2.4. Der Verfügungsberechtigte bzw. Absender (hier das Opfer) hat regelmäßig weder Kenntnis über die Infizierung seines Geräts noch über die durch die Angreifer gesteuerte Datenübermittlung oder die Umleitung des Datenverkehrs an den Sinkhole-Server des IT-Sicherheitsforschenden. Die Datenübermittlung geschieht ohne Beteiligung und ohne willentliche Bestimmung des Opfers. Mithin handelt es sich gerade nicht um einen Fall der nichtöffentlichen Datenübermittlung i.S.d. § 202b Abs. 1 StGB. Mithin ist eine Strafbarkeit der IT-Sicherheitsforschenden nach § 202b Abs. 1 StGB nach der hier vertretenen Meinung i.d.R. ausgeschlossen.

2.3.2.6 Vorbereitung einer Computerstraftat, § 202c Abs. 1 Nr. 2 StGB

Darüber hinaus kann eine Strafbarkeit des IT-Sicherheitsforschenden nach § 202c Abs. 1 Nr. 2 StGB in dem hier diskutierten Fall nach der hier vertretenen Meinung i.d.R. ausgeschlossen werden. Hiernach macht sich strafbar, wer eine Straftat nach § 202a oder § 202b StGB vorbereitet, indem er Computerprogramme *verwende*t, deren Zweck die Begehung solcher Taten ist. Die Computerprogramme, die von dem IT-Sicherheitsforschenden zur Durchführung der Updateinstallation mit anschließender Entfernung der Schadsoftware auf dem jeweiligen Gerät verwendet werden, sind solche, die erst durch eine missbräuchliche Anwendung zu einem Tatwerkzeug werden.[185] Eine bloße Eignung der Softwareprogramme zur Begehung einer Straftat nach § 202a oder § 202b StGB genügt jedoch nicht.[186] Unterstellt, der IT-Sicherheitsforschende würde im Rahmen des vorgenannten Vorgehens dasselbe Computerprogramm wie die Angreifer nutzen, so würde abermals eine Strafbarkeit nach § 202c Abs. 1 Nr. 2 StGB am mangelnden Vorsatz scheitern, denn der hier zu unterstellende „gutwillige Umgang" des IT-Sicherheitsforschenden soll gerade nicht in den Anwendungsbereich des § 202c Abs. 1 StGB fallen.[187]

3. Völkerrechtliche Aspekte

Das Völkerrecht regelt die Beziehungen zwischen Staaten und anderen Völkerrechtssubjekten. Die Handlungen von Privatpersonen im Cyberraum werden grundsätzlich nicht beachtet.[188] Ein Völkerrechtsverstoß liegt grundsätzlich nur dann vor, wenn die betreffende Tat einem Staat zugerechnet werden kann.[189] Das ist der Fall, wenn die Tat von Staatsorganen, Personen die nach nationalem Recht dazu ermächtigt wurden hoheitliche Gewalt auszuüben oder Personen unter staatlicher Steuerung oder Kontrolle begangen wird.[190] Auch die nachträgliche Anerkennung oder Adoption privater Handlungen durch einen Staat führen zur Zurechnung.[191]

Um im Rahmen des völkerrechtlichen Diskurses auf den rechtssicheren Einsatz von Cyberabwehrmaßnahmen hinwirken zu können, bedarf es – als grundlegende

[185] BT-Drs. 16/3656, S. 18; *Eisele*, in: Schönke/Schröder, StGB, 2019, § 202c Rn. 4.
[186] BT-Drds. 16/3656, S. 19.
[187] BT-Drs. 16/3656, S. 18.
[188] Tallinn Manual 2.0, Rule 33, Rn. 1.
[189] Tallinn Manual 2.0, Rule 33, Rn. 2.
[190] Tallinn Manual 2.0, Rules 15, 17.
[191] Tallinn Manual 2.0, Rule 17, Rn. 15 ff.

Voraussetzung – einer Schärfung des Verständnisses für die Begriffe der Passiven und Aktiven Cyberabwehr sowie der mit diesen Begriffen verbundenen Maßnahmen.[192]

3.1 Begriffsabgrenzungen

3.1.1 Passiv vs. aktiv

Maßnahmen der **passiven Cyberabwehr** sind solche, die präventiv ergriffen werden, ohne dass ein konkreter Cyberangriff absehbar ist. Währenddessen sind Maßnahmen der **aktiven Cyberabwehr** solche, die reaktiv ergriffen werden, wenn ein konkreter Cyberangriff unmittelbar und absehbar bevorsteht oder bereits begonnen hat.

3.1.2 Intern vs. extern

Die beiden Formen der Cyberabwehr lassen sich in Bezug auf ihren Wirkungsbereich weiter differenzieren: Maßnahmen, die der Abwehr von Cyberangriffen dienen, können entweder auf die zu verteidigenden IT-Infrastrukturen beschränkt sein und daher **intern** stattfinden, oder Auswirkungen haben, die über diese IT-Infrastrukturen hinausgehen und daher **externer** Natur sein beziehungsweise (zusätzlich) extern wirken.[193]

3.1.3 Nicht intrusiv vs. intrusiv

Darüber hinaus können Maßnahmen mit (zusätzlich) externer Wirkung dahingehend unterschieden werden, ob die Maßnahmen intrusiv oder nicht intrusiv sind. Maßnahmen mit (zusätzlich) externer Wirkung sind **intrusiv**, wenn es aufgrund der Maßnahmen zu einem unbefugten Zugriff auf IT-Anwendungen, -Systeme oder -Infrastrukturen oder die Beeinträchtigung ihrer Vertraulichkeit, Integrität oder Verfügbarkeit kommt beziehungsweise der Versuch hierzu unternommen wird, definiert das US-Institut für Normung NIST.

Nicht-intrusiv sind Maßnahmen mit (zusätzlich) externer Wirkung hingegen dann, wenn sie kein Eindringen in die IT-Anwendungen, -Systeme oder -Infrastrukturen des Angreifers erfordern und auch nicht die Vertraulichkeit, Integrität oder Verfügbarkeit dieser beeinträchtigen, für die Haya Shulman und Michael Waidner Beispiele nennen.[194]

3.1.4 Kategorisierung beispielhafter Maßnahmen

Die nachfolgende Auflistung[195] gibt Beispiele für Maßnahmen der verschiedenen Formen passiver und aktiver Cyberabwehr:

Maßnahmen der Passiven Cyberabwehr mit interner Wirkung

- Einfache Benutzerauthentifizierung, z. B. durch ein Passwort, ohne weitere Konsequenzen bei mehreren Fehlversuchen der Passworteingabe

[192] Das vorliegende Kapitel ist zuerst hier erschienen und wurde nachfolgend wortwörtlich übernommen: https://background.tagesspiegel.de/cybersecurity/ begriffsverwirrung-verhindern-was-massnahmen-aktiver-cyberabwehr-sind-und-was-nicht.
[193] *Denning/Strawser*, Active Cyber Defense: Applying Air Defense to the Cyber Domain, in *Perkovich/Levite*, Understanding Cyber Conflict. Fourteen Analogies, 2017, Nr. 193210.
[194] *Shulman/Waidner*, Der Weg zur aktiven Cyberabwehr, FAZ 2022, über: https://www.faz.net/pro/d-economy/cybersicherheit-der-weg-zur-aktiven-cyberabwehr-17980091.html.
[195] *Gärtner*, Towards a Taxonomy of Cyber Defence in International Law, GI Informatik 2023, S. 474.

- Sichere Passwörter
- Benutzerschulungen

Maßnahmen der Passiven Cyberabwehr mit (zusätzlicher) externer Wirkung

- Austausch von Bedrohungsinformationen, z. B. zwischen Strafverfolgungsbehörden und kommerziellen Dienstleistern (nicht-intrusive Maßnahme[196])
- Kontinuierliches Abfangen von Cyber-Bedrohungen (intrusive Maßnahme[197])
- Präventives Abschwächen der Cyber-Fähigkeiten von Angreifern (intrusive Maßnahme[198]).

Maßnahmen der aktiven Cyberabwehr mit interner Wirkung

- Benutzerauthentifizierung inkl. Reaktionen auf fehlgeschlagene Authentifizierung (z. B. Sperrung des Accounts)
- Behebung von Schwachstellen in den verteidigten IT-Infrastrukturen
- Bewusste (Fehl-)Konfiguration eines IT-Systems, die im Falle eines Angriffs als Köder wirkt und den Angreifer von kritischen IT-Ressourcen weglockt, den Angriff verlangsamt oder Vorwarnungen gibt.

Maßnahmen der aktiven Cyberabwehr mit (zusätzlich) externer Wirkung

- Wiederherstellung eines durch einen Cyberangriff umgeleiteten Datenflusses (nicht-intrusive Maßnahme)
- Zufällige Änderungen der IP-Adresse des Opfers eines Cyberangriffs durch den Verteidiger, um den Cyberangriff zu erschweren (nicht-intrusive Maßnahme[199])
- (Vorübergehende) Unterbrechung oder Übernahme der IT-Infrastruktur des Angreifers, um einen Angriff zu stoppen (intrusive Maßnahme).

3.2 Völkerrechtliche Relevanz der Begriffsabgrenzung

Die Taxonomie stellt den ersten Versuch einer völkerrechtlichen Erfassung von Cyberabwehrmaßnahmen dar. Völkerrechtlich ist sie in zweierlei Hinsicht relevant. Da zur Cyberabwehr, trotz ihrer gegenteiligen Motivation, teils dieselben Techniken genutzt werden wie für Cyberangriffe, hilft die Kategorisierung festzustellen, ob ein gegebener Cyberangriff völkerrechtswidrig ist. Andererseits erlaubt sie einzuordnen, welche Cyberabwehrmaßnahmen rechtlich zulässig sein könnten. Einer definitiven juristischen Beurteilung steht allerdings im Wege, dass die genaue Anwendung der einschlägigen völkerrechtlichen Regeln im Cyberraum derzeit noch umstritten ist.

Methoden der Cyberabwehr dürfen jedenfalls nicht gegen das Gewalt- oder Interventionsverbot verstoßen.[200] Ein Staat darf also weder Gewalt auf dem Territorium eines fremden Staates ausüben noch in seine inneren Angelegenheiten eingreifen. Darüber hinaus ist strittig, ob unterhalb dieser Grenzen bereits die Verletzung staatlicher Souveränität an sich völkerrechtswidrig ist: Während Kritiker Souveränität lediglich als

[196] *Denning/Strawser*, Active Cyber Defense: Applying Air Defense to the Cyber Domain, in *Perkovich/Levite*, Understanding Cyber Conflict. Fourteen Analogies, 2017, Nr. 193210.
[197] U. S. Cyber Command, Achieve and Maintain Cyberspace Superiority, 2018, über: https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20 April%202018.pdf, accessed 29/04/2023.
[198] U. S. Cyber Command, Achieve and Maintain Cyberspace Superiority, 2018, über: https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20 April%202018.pdf, accessed 29/04/2023.
[199] Dewar, R. S.: Active Cyber Defense. CSS Cyber Defence Trend Analysis 1. Center for Security Studies (CSS), 2017, S. 8.
[200] Zur Anwendbarkeit im Cyberraum: Tallinn Manual 2.0, Rule 69, Rn. 1(Gewaltverbot); Rule 66 (Interventionsverbot).

unverbindliches Leitprinzip verstehen,[201] erkennt der überwiegende Teil der Staatengemeinschaft[202] sowie Literatur[203] das Konzept als eigenständige Rechtsnorm an. Folgt man dieser Auffassung, stellt sich die Frage, ab welcher Schwelle Cyberaktivitäten eine Souveränitäts- und damit Völkerrechtsverletzung herbeiführen. Einerseits wird auf einen physischen Schaden, einen Funktionsverlust oder einer Anmaßung staatlicher Befugnisse abgestellt.[204] Nach anderer Ansicht genügt jede unerlaubte, intrusive Handlung im Cyberraum eines Staates.[205]

Ein verbindliches Souveränitätsprinzip zöge eine Einschränkung der zulässigen passiven Cyberabwehrmaßnahmen nach sich; dies ist umso mehr der Fall, wenn man auf eine notwendige Mindest-Eingriffsintensität verzichtet. Während interne sowie externe, nicht-intrusive Handlungen regelmäßig unbeachtlich sein dürften, ist für externe, intrusive Cyberabwehr relevant, ob etwa ein Abfangen oder Abschwächen gegnerischer Cyberfähigkeiten die definierte Schwelle der Souveränitätsverletzung überschreitet. Wenn man jede Intrusion als Souveränitätsverletzung interpretiert, bliebe kein legaler Raum für passive, intrusive Cyberabwehr.

Spiegelbildlich zeigt sich auf Ebene der aktiven Cyberabwehr, dass interne sowie externe, nicht-intrusive Reaktionen auf Cyberangriffe i.d.R. zulässig sein dürften. Für die Beurteilung der Rechtmäßigkeit von aktiven, intrusiven Cyberabwehrmaßnahmen ist abermals entscheidend, ob und inwieweit eine Souveränitätsnorm besteht. Denn auf einen völkerrechtswidrigen Cyberangriff stehen staatlichen Cybersicherheitsakteuren weitreichendere Reaktionsmöglichkeiten – in Form von Gegenmaßnahmen oder gar einem Selbstverteidigungsrecht – zu.[206] Folglich können normalerweise unzulässige Cyberabwehrmaßnahmen im Zuge einer Art digitalen Notwehr rechtmäßig sein.

Ergo hängt die rechtliche Beurteilung intrusiver Cybersicherheitsmaßnahmen vom Bestehen und Reichweite einer Souveränitätsnorm ab. Dessen ungeachtet können aus der Kategorisierung juristisch einordbare Archetypen von Cybersicherheitsmaßnahmen entwickelt werden, wobei v.a. die Klassifizierung einer Handlung als (passiv oder aktiv) intrusiv rechtliche Konsequenzen nach sich zieht.

4. Fazit & Handlungsempfehlungen

Aktive Cyberabwehr ist unabdingbar, um die Gesellschaft und ihre kritischen Infrastrukturen vor akut drohenden Cyberangriffen zu schützen. Zur Fortentwicklung der aktiven Cyberabwehr durch IT-Sicherheitsforschende ist Rechtssicherheit unumgänglich.

4.1 Zum strafrechtlichen Rahmen

Der Beitrag hat zunächst aufgezeigt, dass es bei der Abwendung eines BGP-Hijacking-Angriffs und der Wiederherstellung des ursprünglich intendierten Routings ein rechtliches

[201] *Wright für die Regierung Großbritanniens*, Cyber and International Law in the 21st Century.
[202] *NATO Standardization Office*, NATO Allied Joint Doctrine for Cyberspace Operations; *Außenminister der Niederlande*, Letter to the parliament on the international legal order in cyberspace, Appendix: International law in cyberspace; *Regierung von Finnland*, International Law and Cyberspace; *Regierung von Neuseeland*, The Application of International Law to State Activity in Cyberspace; *Regierung von Frankreich*, International Law Applied to Operations in Cyberspace.
[203] *Corn/Taylor*, AJIL 2017, 207.
[204] Tallinn Manual 2.0, Rule 4, Rn. 10.
[205] *Roguski*, Opinio Juris 2019.
[206] Tallinn Manual 2.0, Rule 19, Rn. 1, 11 ff.

Risiko für IT-Sicherheitsforschende gibt, sich (insbesondere) gem. § 303 a StGB strafbar zu machen.

Handlungsempfehlung 1
Um dieses Risiko für IT-Sicherheitsforschende auszuschließen ist es grundsätzlich ratsam – sofern möglich – bereits vor der Durchführung der Verteidigungsmaßnahme, das Einverständnis des Providers und des Angegriffenen einzuholen.

Aufgrund der Tatsache, dass es bei Maßnahmen der aktiven Cyberabwehr i.d.R. dringend erforderlich ist, dass diese schnellstmöglich durchgeführt werden, um schwerwiegende Auswirkungen der Cyberangriffen erfolgreich zu verhindern, bzw. schnellstmöglich stoppen zu können, wird die Einholung einer Einwilligung allerdings regelmäßig zu lange dauern und daher praxisfern sein. Das Institut der mutmaßlichen Einwilligung des verfügungsbefugten Providers kann in dem hier besprochenen Szenario des BGP-Hijacking Abhilfe verschaffen und eine Strafbarkeit des IT-Sicherheitsforschenden i.d.R. ausschließen. Spätestens über den rechtfertigenden Notstand besteht jedoch i.d.R. eine Rechtfertigungsmöglichkeiten.

Handlungsempfehlung 2
Um eine Strafbarkeit der IT-Sicherheitsforschende bestmöglich zu vermeiden, gilt es eine enge Zusammenarbeit mit den IT-Sicherheitsforschenden und Providern bzw. Betreibern der externen BGP-Router zu etablieren.

Handlungsempfehlung 3
Auch wenn die mutmaßliche Einwilligung i.d.R. zu bejahen sein wird, ist zu empfehlen, das Vorgehen der IT-Sicherheitsforschenden zu dokumentieren bspw. durch ein unveränderbares Protokoll sowie eine nachträgliche Meldung gegenüber dem verfügungsberechtigten Provider und dem Angegriffenen umzusetzen.

Unter der Annahme der in diesem Beitrag dargestellten Methode der Abkoppelung oder Übernahme von für Angriffe genutzten Netzwerk-Ressourcen scheint ein rechtliches Risiko für IT-Sicherheitsforschende aus Sicht der Autoren derzeit nicht absehbar. Das liegt zunächst daran, dass die vorgenommenen Maßnahmen der IT-Sicherheitsforschenden sich zunächst darauf beschränken, die Verantwortlichen oder den Betreiber des jeweiligen DNS-Servers über Sicherheitsrisiken und die Detektion von Schadprogrammen zu informieren. Sofern nach positiver Auswertung der Sicherheitswarnung eine Anpassung der DNS-Einträge und Weiterleitung vorgenommen wird, so findet eine hierdurch begangene strafrechtlich relevante Tathandlung der Datenveränderung i.S.d. § 303a Abs. 1 StGB eigenständig und ohne Zutun der IT-Sicherheitsforschenden durch die Verantwortlichen oder DNS-Betreibern statt. Das anschließende Empfangen, Speichern erfüllt keinen Straftatbestand des StGB.

Handlungsempfehlung 4
Wenngleich ein rechtliches Risiko für IT-Sicherheitsforschende im Rahmen der vorstehenden Methode aus Sicht der Autoren derzeit nicht absehbar scheint, ist dennoch eine Dokumentation über das konkrete Vorgehen und die Absichten der IT-Sicherheitsforschenden zu empfehlen. Auch die Vorteile einer Zusammenarbeit mit sowie die Weitergabe der gesammelten Informationen an die zuständigen Behörden sollte (neben ggf. bestehender rechtlicher Verpflichtungen zur Zusammenarbeit mit diesen Stellen) u.a. zum Zwecke der Opferidentifizierung und der Vornahme etwaig erforderlicher Sicherheitsvorkehrungen erwogen werden – hierfür kann die zuvor genannte Dokumentation gleichfalls hilfreich sein.

Schließlich ergibt sich bei der Beseitigung von Schwachstellen und Schadsoftware auf den Systemen der Opfer ein strafrechtliches Risiko für IT-Sicherheitsforschende vornehmlich aus § 303a Abs. 1 StGB.

Handlungsempfehlung 5
Um eine Strafbarkeit der IT-Sicherheitsforschenden zu vermeiden, ist es grundsätzlich ratsam, bereits vor Durchführung der Verteidigungsmaßnahme eine Risikoabschätzung durchzuführen und analog Handlungsempfehlung 1 – sofern möglich – das Einverständnis des Angegriffenen einzuholen. Ist die Umsetzung der Cybermaßnahme jedoch besonders zeitkritisch und ein schnellstmögliches Handeln des IT-Sicherheitsforschenden dringend erforderlich, um schwerwiegende Auswirkungen zu verhindern oder stoppen, steht das Einholen einer Einwilligung regelmäßig im Widerspruch zur Dringlichkeit der Verteidigungsmaßnahme. In diesen Fällen besteht die Handlungsempfehlung aus Sicht der Autoren zumindest in der Anfertigung einer abgeschwächten Risikoabschätzung bzw. einer Dokumentation über die durchgeführten Maßnahmen sowie die damit verfolgten Ziele, um im Einzelfall die Gründe für die Bejahung einer mutmaßlichen Einwilligung sowie das Vorliegen der Merkmale des rechtfertigenden Notstands gemäß § 34 StGB darlegen zu können.
Um die betroffenen Opfer über die Infizierung ihres Geräts zu informieren und ihnen die Möglichkeit zu geben, ggf. erforderliche Sicherheitsvorkehrungen zu treffen, ist eine Mitteilung der von den Forschenden gesammelten Daten an die zuständigen Stellen (neben ggf. bestehender rechtlicher Verpflichtungen zur Zusammenarbeit mit diesen Stellen) zur Opferidentifizierung zu erwägen.

Es bleibt zu betonen, dass die Betrachtung der drei genannten Methoden offensiver Cyberabwehr ausschließlich aus Sicht des deutschen Strafrechts vorgenommen wurde.

4.2 Zum völkerrechtlichen Rahmen

Die Handlungen von Privatpersonen im Cyberraum werden grundsätzlich nicht im Völkerrecht beachtet, da ein Völkerrechtsverstoß grundsätzlich nur vorliegt, wenn die betreffende Tat einem Staat zugerechnet werden kann. Vor diesem Hintergrund lassen sich folgende Empfehlungen für IT-Sicherheitsforschende herleiten.

Handlungsempfehlung 6
In dem Fall, dass IT-Sicherheitsforschende mit der Verteidigung und Sicherung von staatlichen IT-Infrastrukturen beauftragt werden, empfiehlt es sich die zu erfüllenden Aufgaben zunächst genau zu definieren.

Handlungsempfehlung 7
Darüber hinaus sollten IT-Sicherheitsforschende bewerten, ob es im Rahmen ihrer beauftragten Tätigkeit zu (unbeabsichtigten) Intrusionen in oder Schäden an ausländischen IT-Infrastrukturen kommen könnte.

Handlungsempfehlung 8
Sowohl das Ergebnis der Aufgabendefinition als auch die Bewertung möglicher (unbeabsichtigter) Intrusionen in oder Schäden an ausländischen IT-Infrastrukturen sollten dem Auftraggeber vor Umsetzung der Verteidigung- und/oder Sicherungshandlungen vorgelegt werden und von ihm gebilligt werden.

Handlungsempfehlung 9
Für den Fall, dass die vorgenannten Handlungsempfehlungen aus zeitlichen Gründen nicht eingehalten werden können, z. B. in einem akuten Notfall, kann es ratsam sein, noch vor Vorliegen eines solchen Akutfalls zumindest allgemeine Hinweise über

mögliche Risiken auszuformulieren und den Auftraggebern vor der Umsetzung der Notfallmaßnahmen zur Kenntnisnahme vorzulegen. Um in einem solchen Fall die vorgenommenen Handlungen nachvollziehen zu können, sollte zudem nach Durchführung der Notfallmaßnahmen eine Dokumentation der wichtigsten Rahmenbedingungen der erfüllten Aufgaben erstellt werden (u.a. welche Maßnahmen genau vorgenommen wurden, inwiefern diese Maßnahmen Auswirkungen auch außerhalb deutscher IT-Infrastrukturen haben und ob [für die IT-Sicherheitsforschenden erkennbar] Intrusionen oder Schäden vorgefallen sind).

Der Grund hierfür ist, dass auch Taten, die in Überschreitung der eingeräumten Befugnisse begangen werden, dem beauftragenden Staat zugerechnet werden und somit zu dessen völkerrechtlichen Verantwortlichkeit führen.[207] Auf diesem Wege könnten sich eventuelle, spätere Vorwürfe im Auftragsverhältnis zum Staat vermeiden lassen, auch wenn ein Völkerrechtsverstoß keine direkten Konsequenzen für die IT-Sicherheitsforschenden haben wird.

4.3 Gesamtschau

IT-Sicherheitsforschende sollten sich bereits vor der Umsetzung von Maßnahmen aktiver Cyberabwehr – seien sie staatlich, in sonstiger Weise oder nicht beauftragt – mit dem relevanten Rechtsrahmen auseinandersetzen. Hierbei ist regelmäßig der individuelle Einzelfall zu berücksichtigen, so dass die vorliegende Ausarbeitung nur einen ersten Überblick über das Thema geben kann.

IT-Sicherheitsforschende sollten sich dessen bewusst sein, dass ihre in Deutschland vorgenommenen Handlungen im Cyberraum auch gegen das Recht, insbesondere das Strafrecht, anderer Staaten verstoßen könnten, sollten sie dort Auswirkungen entfalten.[208] Auch dieser Umstand – sowie ggf. die Ungewissheit über die geografische „Verortung" der Auswirkungen des eigenen Handelns (das im Cyberraum erfolgt) sowie zeitliche Implikationen der durch IT-Sicherheitsforschende durchgeführten Maßnahmen (z.B. ggf. fehlende Zeit zum Einholen von Einwilligungen oder zur Identifizierung der im konkreten Einzelfall vorliegenden Risiken) – sollte in der Auseinandersetzung mit dem relevanten Rechtsrahmen Berücksichtigung finden.

[207] Tallinn Manual 2.0, Rule 15, Rn. 12.
[208] Tallinn Manual 2.0, Rule 9, Rn. 5, 12.

ATHENE
Nationales Forschungszentrum
für angewandte Cybersicherheit