Research Honeypots – Strafbarkeitsrisiken für IT-Sicherheitsforschende?

von PD Dr. Georgia Stefanopoulou, L.L.M.[*]

Abstract
Eine in der IT-Sicherheit eingesetzte Technik zur Analyse von Cyberangriffen und zur Detektion von Sicherheitslücken sind sog. honeypots. Dabei handelt es sich um Rechnernetz-Simulationen, die absichtlich mit Schwachstellen versehen sind, um Angreifer anzulocken. Hackertaktiken können dann beobachtet und studiert werden. Werden Honeypots bei der Analyse und Bekämpfung von sog. D[R]DoS-Attacken eingesetzt, entsteht folgende Besonderheit: Erst durch den Honeypot wird der Angriff möglich. Dies wirft die Frage auf, ob sich IT-Forschende wegen Beihilfe zu den Straftaten des Cyberangreifers strafbar machen. Mit dieser Frage befasst sich der vorliegende Beitrag.

Honeypots are a technique used in IT security to analyse cyber attacks and detect security vulnerabilities. These are computer network simulations that are deliberately designed with weak points so that they can attract attackers. Hacker tactics can then be observed and studied. If honeypots are used to analyse and combat so called D[R]DoS attacks, the following peculiarity has to be taken into account: the attack is only made possible by the honeypot. This raises the question of whether IT researchers are liable to prosecution for aiding and abetting the cyber attacker's criminal offences. This article deals with this question.

I. Einleitung

„Da ist der Hacker. Und da bin ich. […] Da ist der Köder. Na komm, beiß schon an! […] Ha! Er hat den Haken geschluckt! Der Kuckuck hat seine Eier in das falsche Nest gelegt.“[1] So beschreibt der US-Amerikaner *Clifford Stoll* in seinem Sachbuchklassiker zum Computerhacking – „Kuckucksei“ – die ersten Momente seines Erfolgs gegen die Spione in dem Computernetzwerk des Lawrence Berkeley National Laboratory Ende der achtziger Jahre. Den Erfolg brachte nach einer langen Spurensuche der Einbau einer Falle. *Stoll*, der derjenige war, der aufgrund eines Abrechnungsfehlers im System als erster die Computereinbrüche bemerkte, berichtet über die Einrichtung eines fiktiven Netzwerks mit vielen Informationen über erfundene Militärbasen, vermeintliche Sergeants und Colonels.[2] Dieses fiktive Netzwerk lockte die nach militärischen Geheimnissen suchenden Hacker so lange an, wie es nötig war, um ihre Langzeitverbindungen zu verfolgen und sie schließlich in Hannover zu lokalisieren.

Die Überlistungseinrichtung, die Stoll Ende der Achtziger einsetzte, als „Computerpiraterie“[3] und Computersicherheit noch in ihren Anfängen waren, ist heute eine in der IT-Sicherheit etablierte und mit einer bildhaften Bezeichnung versehene Technik: *honeypot*. Eine Rechnernetz-Simulation mit fiktiven Daten, bei der bewusst schwache Stellen eingebaut sind, soll bei Hackern so ablenkend bzw. verlockend wirken wie ein Topf mit Honig bei Bären. Damit sollen Angriffe auf das echte Netzwerk vermieden, Angriffe in der kontrollierten Umgebung des simulierten Netzwerks beobachtet und Eindringlinge identifiziert werden. Sog. *product honeypots* bieten sich als Bestandteil einer effektiven IT-Sicherheitsstrategie von Unternehmen an. Man kann nicht nur gegenwärtige Angriffe rechtzeitig bemerken, sondern, indem man die Taktiken der Angreifer beobachtet, auch Sicherheitslücken schließen und sich für zukünftige Gefährdungen besser ausrüsten.

Gerade diese letzte Möglichkeit, Cyberangriffe innerhalb der simulierten Umgebung zu studieren und damit Sicherheitsvorkehrungen zu verbessern, macht den Einsatz von Honeypots auch für IT-Sicherheitsforschende attraktiv.[4] In diesem Zusammenhang spricht man von sog. *research honeypots*. Absichtlich verwundbare Systeme werden als Attrappen verwendet, damit Angriffsmuster analysiert werden können.[5] Eingesetzt werden sie unter anderem bei der Analyse und Bekämpfung von sog. D[R]DoS-Attacken (Distributed[-Reflected]-Denial-of-Service-Angriffen).[6]

Mit Blick auf dieses Anwendungsfeld von Research Honeypots wird in der noch eher übersichtlichen Literatur zum Thema diskutiert, ob durch diese Methode Strafbarkeitsrisiken für IT-Forschende entstehen. Da der Honeypot „Bestandteil des Angriffs“[7] werden kann, kommt nach einer Ansicht Strafbarkeit wegen Beihilfe zu den Straftaten in Betracht, die mit D[R]Dos-Attacken in Verbindung stehen.[8] Über diese Auffassung wird im Folgenden auf dem Boden der Beteiligungsdogmatik nachgedacht.

---

* *PD Dr. Georgia Stefanopoulou* vertritt im Sommersemester 2024 den Lehrstuhl für Strafrecht, Strafprozessrecht, Internationales Strafrecht, Strafrechtsvergleichung und Rechtsphilosophie an der Universität Leipzig.

1 *Stoll*, Kuckucksei. Die Jagd auf die deutschen Hacker, die das Pentagon knackten, 1996, S. 302 f., 308.

2 *Stoll* (Fn. 1), S. 296.

3 So *Stoll* (Fn. 1), S. 423.

4 *Wörner/Blocher*, in: Golla/Brodowski, IT-Sicherheitsforschung und IT-Strafrecht, 2023, S. 57 (72).

5 *Böken*, in: Kipker, Cybersecurity, Rechtshandbuch, 2. Aufl. (2023), 19. Kap. Rn. 83; *Wörner/Blocher* (Fn. 4), S. 72.

6 *Böken*, in: Kipker, 19. Kap., Rn. 84; *Wörner/Blocher* (Fn. 4), S. 72; *Vogelgesang/Möllers/Potel*, MMR 2017, 291 ff.

7 *Böken*, in: Kipker, Cybersecurity, 19. Kap. Rn. 84.

8 *Vogelgesang/Möllers/Potel*, MMR 2017, 291 (294); *Wörner/Blocher* (Fn. 4), S. 72 ff.

Am Beispiel des Betreibens von Honeypots wird außerdem gezeigt, dass digitale Vorgänge nicht einfach in die herkömmlichen dogmatischen Schemata hineingezwängt werden können. Dies bedeutet nicht, dass etablierte und ausdifferenzierte Begriffe und Strukturen aufgegeben werden müssen. Sie sollten nur nicht ohne Anpassung an die Besonderheiten von digitalen Vorgängen angewandt werden. Damit ist generell die Aufgabe des sog. Internet- bzw. Computerstrafrechts angesprochen: dass unter Berücksichtigung der Besonderheiten digitaler Vorgänge Lösungen erarbeitet werden, die an die Spezifizitäten des digitalen Phänomenbereichs angepasst sind. Diese Vorgehensweise empfiehlt sich auch bei der Frage der Strafbarkeit von Research Honeypots. Das uns zur Verfügung stehende Instrumentarium der Teilnahmelehre ist an die Besonderheiten digitaler Abläufe anzupassen und so auf das konkrete Problem anzuwenden.

II. Betreiben von Honeypots als strafbare Teilnahme an den Straftaten des D[R]DoS-Angreifers?

1. Kritische Würdigung der Ansichten im Schrifttum

Bei den D[R]DoS-Angriffen wird gezielt die Internetverbindung des Opfers durch die Zusendung einer Flut von Daten (Zusendung einer Vielzahl von Anfragen) überlastet, so dass die Kontaktaufnahme mit dem Server bzw. der Webseite unmöglich wird.[9] D[R]DoS-Attacken sind wegen Datenunterdrückung nach § 303a StGB strafbar und auch gem. § 303b Abs. 1 Nr. 2 StGB (eingeführt durch das 41. StrÄndG vom 7.8.2007[10]) als Computersabotageakt erfasst.[11] Da der Täter die Lähmung der Internetverbindung oft mit Erpressungsabsicht vornimmt – der D[R]DoS-Angriff soll nach Zahlung eines Lösegeldes beendet werden –, ist in diesen Fällen auch § 253 StGB erfüllt.[12] Die Überlastung der Internetverbindung von Online-Shops und anderen groß angelegten Webseiten, die gerade für eine hohe Zahl von Besucher:innen errichtet sind, lässt sich allerdings nicht allein durch Datenpakete erreichen, die durch einen einzelnen Server geschickt werden.[13] Der Zugang zu größeren Webseiten kann erst versperrt werden, wenn der Angreifer sog. *Amplifier* einsetzt, d.h. Internetdienste, die die Datenvolumen vergrößern.[14] Die Anziehungskraft von Honeypots als Lockmittel besteht darin, dass sie sich als Amplifier einsetzen lassen.[15] Werden sie entdeckt, können sie zur Durchführung eines Angriffs verwendet werden.[16] Forschende können so neue Angriffstechniken und Angriffstools beobachten und studieren.

Das strafrechtsdogmatische Problem, das sich hierbei stellt, springt gleich ins Auge. IT-Forschende, die Honeypots Cyberkriminellen gezielt zur Verfügung stellen, wirken an sich daher an tatbestandsmäßigen rechtswidrigen Haupttaten anderer mit – sie „setzen sich mithin ‘in das Boot’ jener Angreifer“[17]. Das Betreiben eines Honeypots könnte daher möglicherweise als strafbare Teilnahme einzustufen sein. Dabei wird eine Teilnahme in Form der Anstiftung in der Literatur zu Recht schnell abgelehnt.[18] Geht man von der herrschenden Kommunikationstheorie[19] aus, liegt ein Bestimmen im Sinne des § 26 StGB nicht vor.[20] Durch Einrichten eines Honeypots schafft der Betreiber zwar eine verführende Situation, die kausal den Tatentschluss hervorruft, es fehlt jedoch an einem geistigen Kontakt zwischen ihm und der Täter:in des D[R]DoS-Angriffs.[21] Es verhält sich hier nicht anders als beim klassischen Lehrbuchbeispiel, bei dem der Provokateur P an einem für den Täter T gut erreichbaren Ort Geldscheine deponiert, um T wegen Diebstahls überführen zu können. Ein kommunikatives Einwirken auf T, das die Bestrafung des Provokateurs „gleich einem Täter“ rechtfertigen könnte, liegt nicht vor.[22] Auch zwischen dem Honeypot-Betreiber und dem D[R]DoS-Angreifer besteht keine kommunikative Beziehung.[23]

Kann man Teilnahme in Form der Anstiftung relativ zügig ablehnen, gilt dies nicht für die Beihilfe. Hier gibt es mehr Diskussionsbedarf. Einer Ansicht nach ist das Betreiben von Honeypots zur Analyse von D[R]DoS-Attacken als vorsätzliche Beihilfe zur Computersabotage zu bewerten.[24] Das Betreiben des Honeypots ermögliche objektiv durch die Verstärkung der Datenvolumen und die Weiter-

---

9 *Kochheim*, Cybercrime und Strafrecht in der Informations- und Kommunikationstechnik, 2. Aufl. (2018), S. 270; *Hilgendorf*, in: SSW-StGB, 5. Aufl. (2021), § 303b Rn. 10; s. auch *Hilgendorf/Kusche/Valerius*, Computer-und Internetstrafrecht, 3. Aufl. (2023), Rn. 414, 433.

10 BGBl. I, S. 1786 (Umsetzung des Übereinkommens des Europarats über Computerkriminalität und der Umsetzung des Rahmenbeschlusses 2005/222/JI des Rates vom 24. Februar 2005 über Angriffe auf Informationssysteme [ABl. EU Nr. L 69 S. 67]).

11 *Hilgendorf*, in: SSW-StGB, § 303b Rn. 10; s. auch *Hilgendorf/Kusche/Valerius*, Computer- und Internetstrafrecht, Rn. 414, 592; *Kochheim* (Fn. 9), S. 270.

12 *Wörner/Blocher* (Fn. 4), S. 73.

13 *Böken*, in: Cybersecurity, Kipker, 19. Kap. Rn. 84; *Vogelgesang/Möllers/Potel*, MMR 2017, 291 (292).

14 *Böken*, in: Kipker, Cybersecurity, 19. Kap. Rn. 84; *Vogelgesang/Möllers/Potel*, MMR 2017, 291 (292).

15 *Böken*, in: Kipker, Cybersecurity, 19. Kap. Rn. 84; *Vogelgesang/Möllers/Potel*, MMR 2017, 291 (292).

16 *Böken*, in: Kipker, Cybersecurity, 19. Kap. Rn. 84.

17 *Wörner/Blocher* (Fn. 4), S. 73.

18 *Vogelgesang/Möllers/Potel*, MMR 2017, 291 (293).

19 Dazu *Wessels/Beulke/Satzger*, Strafrecht AT, 53. Aufl. (2023), Rn. 885; *Rengier*, Strafrecht AT, 15. Aufl. (2023), § 45 Rn. 27 ff.

20 *Vogelgesang/Möllers/Potel*, MMR 2017, 291 (293). Zu einem anderen Ergebnis würde man allerdings auf dem Boden der Verursachungstheorie kommen, wonach das bloße kausale Hervorrufen des Tatentschlusses und somit die gezielte Schaffung tatprovozierender Umstände für das Bestimmen ausreichend sind, s. dazu *Rengier*, Strafrecht AT, § 45 Rn 27 ff.; *Wessels/Beulke/Satzger*, Strafrecht AT, Rn. 885. Geht man von der Verursachungstheorie aus, sollte man gleichwohl mit Blick auf einen möglicherweise bereits bestehenden Tatentschluss nicht zu schnell das Bestimmen bejahen (sog. omnimodo facturus). Es sollte den Intentionen der Honeypot-Betreiber doch gerade entgegenkommen, dass ihre Honeypots von bereits zur Tat entschlossenen Tätern gefunden werden, vgl. *Hübner*, Rechtsstaatswidrig, aber straflos? Der agent provocateur-Einsatz und seine strafrechtlichen Konsequenzen, 2020, S. 49. Die Frage der Tatentschlossenheit oder der bloßen Tatgeneigtheit wird außerdem in einer großen Zahl von Fällen mit praktischen Feststellungsschwierigkeiten verbunden sein, *Hübner* (Fn. 20), S. 49.

21 Vgl. *Rengier*, Strafrecht AT, § 45 Rn. 27.

22 *Rengier*, Strafrecht AT, § 45 Rn. 30.

23 *Vogelgesang/Möllers/Potel*, MMR 2017, 291 (293).

24 *Vogelgesang/Möllers/Potel*, MMR 2017, 291 (294); s. auch *Wörner/Blocher* (Fn. 4), S. 73 f., wonach auch eine Beihilfe zur Erpressung in Betracht kommt.

leitung der Informationen zum Server des Opfers den Angriff.[25] Ein Hilfeleisten liege damit vor. Das Betreiben des Honeypots sei auch nicht eine neutrale, berufstypische Handlung ohne deliktischen Bezug, über die ein Zurechnungsausschluss begründet werden könnte, denn die IT-Forschenden intendieren ja gerade den deliktischen Einsatz des Honeypots durch den Haupttäter.[26] Auch die Figuren des erlaubten Risikos und der Sozialadäquanz seien nicht zugunsten der Forschenden heranzuziehen.[27] Bejaht wird auch der Gehilfenvorsatz. Die Argumentation bezieht sich hier zunächst auf die Anforderungen an die Bestimmtheit des Gehilfenvorsatzes, die bekanntermaßen gering sind.[28] Der Vorsatz des Gehilfen muss nicht ein „konkret-individualisiertes Geschehen" erfassen.[29] Daher ist richtig, wenn darauf hingewiesen wird, dass der Vorsatz nicht daran scheitern kann, dass der Honeypot-Betreiber nicht alle Einzelheiten der späteren Haupttat kennt.[30] Ebenso richtig ist, dass der Haupttäter von der Hilfeleistung nicht notwendigerweise Kenntnis haben muss.[31] Fraglicher wird allerdings die Argumentation, wenn sie sich mit den konkreten Motiven der IT-Forschenden auseinandersetzt. Ob sie auf die Verbesserung der IT-Sicherheit abzielen und die Haupttat in der Sache nicht billigen, spielt nach dieser Auffassung keine Rolle.[32] Es komme allein darauf an, ob ihnen bewusst sei, dass ihre Handlung (das Betreiben des Honeypots) geeignet ist, den D[R]DoS-Angriff zu fördern.[33] Mit Blick auf die vergleichbare Problematik des Einsatzes von Lockspitzeln, bei der die Frage der Tatbestandsmäßigkeit des Verhaltens mit Blick auf die mittelbaren Bestrebungen der Ermittler sehr ausdifferenziert behandelt wird, erfolgt die Bejahung des Teilnehmervorsatzes an dieser Stelle etwas zu pauschal.[34]

Die Bejahung des Gehilfenvorsatzes bei einem Honeypot-Einsatz bleibt daher zu Recht in der Literatur nicht unwidersprochen. Die Gegenansicht bezweifelt mit Blick auf den Beschluss des *BVerfG* zu § 202c StGB[35] (Vorbereiten des Ausspähens und Abfangens von Daten) die Richtigkeit des oben dargestellten Ansatzes.[36] So wie der Hackerbegriff zweierlei bedeuten kann – Softwarespezialisten oder Personen, die illegal in Rechnersysteme eindringen –,[37] können auch „Hacker-Tools" auf zweierlei Weise eingesetzt werden: zur Entwicklung von Sicherheitssoftware oder zur Schädigung von Rechnersystemen.[38] Man spricht in diesem Zusammenhang von „dual use tools".[39] Inwieweit diese als Tatobjekt des § 202c StGB erfasst werden können, lasse sich anhand des Zwecks ihrer Entwicklung klären, so das *BVerfG*[40]: „Tatobjekt des § 202c Abs. 1 Nr. 2 StGB kann nur ein Programm sein, dessen Zweck die Begehung einer Straftat nach § 202a StGB (Ausspähen von Daten) oder § 202b StGB (Abfangen von Daten) ist. Danach muss das Programm mit der Absicht entwickelt oder modifiziert worden sein, es zur Begehung der genannten Straftaten einzusetzen. Diese Absicht muss sich ferner objektiv manifestiert haben. Schon nach dem Wortlaut nicht ausreichend wäre, dass ein Programm – wie das für so genannte dual use tools gilt – für die Begehung der genannten Computerstraftaten lediglich geeignet oder auch besonders geeignet ist."[41]

Die Ansicht, wonach das Betreiben von Honeypots keine Beihilfe ist, weist auf die Funktion von IT-Systemen wie Honeypots als „dual-use-Vorrichtungen"[42] hin und wendet die Vorgaben des *BVerfG* in folgender Weise an: Strafbar kann der Einsatz von dual-use-tools nur sein, wenn diese zum Zweck der Schädigung und nicht zu dem legitimen Zweck der Sicherheitsanalyse entwickelt wurden.[43] Diese Leitlinie gelte auch für die Frage, ob ein Beihilfevorsatz vorliegt.[44] Der Einsatz von Honeypots sei ein anerkanntes Mittel zur Verbesserung der IT-Sicherheitsvorkehrungen, das auch in § 7b Abs. 4 BSIG und in § 100 Abs. TKG genannt wird.[45] Sie dienten nicht einem Schädigungszweck, deshalb sei ein Gehilfenvorsatz zu verneinen.[46] Dieser Auffassung ist insoweit zuzustimmen, als sie den Gehilfenvorsatz besonders problematisiert und, anders als die erste Auffassung, auch die ferneren bzw. mittelbaren Bestrebungen der IT-Forschenden berücksichtigt.

Gleichwohl lässt sich erwidern: Aus den Ausführungen des *BVerfG* ergibt sich keine Reduzierung des Schädigungszwecks auf eine eng verstandene Absicht, eine Schädigung herbeizuführen. Erfasst wird auch die Absicht für sich, das Tool zur Begehung von Schädigungen einzusetzen. Der Schädigungszweck ist nicht allein von dem gewünschten Taterfolg her zu definieren, sondern auch durch die zum Erfolg eingesetzten Mittel, d.h. nicht nur vom Endziel der Schädigung her, sondern auch vom Zwischenziel der Missbrauchsgefahrschaffung. Fehlt es zwar

25 *Vogelgesang/Möllers/Potel*, MMR 2017, 291 (293 f.); *Wörner/Blocher* (Fn. 4), S. 73 f.
26 *Wörner/Blocher* (Fn. 4), S. 73 f.
27 *Wörner/Blocher* (Fn. 4), S. 73 f.
28 Statt vieler *Fischer*, StGB, 69. Aufl. (2022), § 27 Rn. 22.
29 Dazu *Rengier*, Strafrecht AT, § 45 Rn. 115.
30 *Vogelgesang/Möllers/Potel*, MMR 2017, 291 (293); *Wörner/Blocher* (Fn. 4), S. 74.
31 *Vogelgesang/Möllers/Potel*, MMR 2017, 291 (293); *Wörner/Blocher* (Fn. 4), S. 75.
32 *Vogelgesang/Möllers/Potel*, MMR 2017, 291 (293); *Wörner/Blocher* (Fn. 4), S. 75.
33 *Wörner/Blocher* (Fn. 4), S. 75.
34 Auf die Ähnlichkeit der Konstellationen weist auch die hier dargestellte Ansicht hin, allerdings nur kurz und allein in Bezug auf Rechtfertigungsfragen, s. *Wörner/Blocher* (Fn. 4), S. 75.
35 *BVerfG*, HRRS 2009 Nr. 560.
36 *Böken*, in: Kipker, Cybersecurity, 19. Kap. Rn. 86.
37 Darauf verweist schon *Stoll* in seinem am Anfang zitierten Report: „Das Wort Hacker hat zwei sehr verschiedene Bedeutungen. Die Leute, die ich kannte und die sich Hacker nannten, waren Softwarespezialisten, die es fertigbrachten, sich auf kreative Weise aus engen Ecken herauszuprogrammieren. […] Im allgemeinen Sprachgebrauch jedoch ist ein Hacker jemand, der in Computer einbricht. […] Softwarespezialisten alten Stils sind stolz auf den Namen Hacker und empört über die Kerle, die sich diesen Namen angeeignet haben.", *Stoll* (Fn. 1), S. 15 f.
38 *Böken*, in: Kipker, Cybersecurity, 19. Kap. Rn. 86.
39 *Krüger/Sorge/Vogelgesang*, in: Schweighofer/Kummer/Saarenpää/Schafer, Datenschutz/Legal Tech, Data Protection/Legal Tech, 2018, S. 529 (531); *Kochheim* (Fn 9), S. 831.
40 *BVerfG*, HRRS 2009 Nr. 560, Rn. 60.
41 *BVerfG*, HRRS 2009 Nr. 560, Rn. 61.
42 *BVerfG*, HRRS 2009 Nr. 560, Rn. 26.
43 *Böken*, in: Kipker, Cybersecurity, 19. Kap. Rn. 86.
44 *Böken*, in: Kipker, Cybersecurity, 19. Kap. Rn. 86.
45 *Böken*, in: Kipker, Cybersecurity, 19. Kap. Rn. 86.
46 *Böken*, in: Kipker, Cybersecurity, 19. Kap. Rn. 86.

im Fall des IT-Forschenden an der Absicht, das Endziel zu erreichen, steht gleichwohl die Missbrauchsgefahrschaffungsabsicht im Hinblick auf ein notwendiges Zwischenziel fest: dass nämlich die Vorrichtung durch andere in schädigender Weise verwendet wird. Die Priorisierung des Endziels bzw. die Unterordnung des unmittelbaren Zwischenziels zur Ablehnung des Schädigungszwecks und des Beihilfevorsatzes erklärt sich nicht ohne weiteres. Einer solchen Priorisierung widerspricht zunächst auch die herkömmliche Bestimmung des strafrechtlichen Absichtsbegriffs, wonach das Streben nach einem notwendigen (Zwischen-)Ziel ausreicht und das Endziel nicht entlastet. Das Sprichwort „Der Zweck heiligt die Mittel" lässt sich bei der Frage des Vorsatzes nicht ohne weiteren Begründungsaufwand verwenden.

2. Die Vollendung als Gegenstand des Vorsatzes

Argumentationshilfe für eine dogmatisch untermauerte Priorisierung des ferneren Ziels der IT-Sicherheit bei der Frage des Gehilfenvorsatzes lässt sich durch die bereits angesprochene Diskussion über die Strafbarkeit des Lockspitzels (agent provocateur) gewinnen. Beim Lockspitzel geht es zwar schwerpunktmäßig um die Bestimmung des Anstiftervorsatzes, die gleichen Vorsatzprobleme stellen sich jedoch auch beim Gehilfenvorsatz.[47] Die Lösungsansätze, die für die Konstellation des Lockspitzels angeboten werden, lassen sich daher auf die Beihilfe und somit auf die Frage der Beihilfestrafbarkeit von Honeypot-Betreibern übertragen. Ausgangspunkt der Überlegungen ist hierbei die in der Strafrechtswissenschaft unstrittige Auffassung, dass der Vorsatz des Teilnehmers stets auf die Vollendung der Haupttat gerichtet sein muss.[48] Will der Teilnehmer die Vollendung der Haupttat nicht oder weiß er, dass ihre Vollendung nicht möglich ist, scheidet die Teilnahme (Anstiftung wie Beihilfe) aus.[49] Damit kommt es für die Frage der Strafbarkeit des Teilnehmers auf die Frage an, was als Vollendung zu verstehen ist. Auch der Gehilfenvorsatz des Honeypot-Betreibers lässt sich nicht ohne Beachtung dieser dogmatischen Kategorie erörtern.[50]

Wendet man sich der Frage zu, was als Vollendung und als Vollendungsvorsatz anzusehen sind, lässt sich eine Lösung bereits auf der Tatbestandsebene finden, ohne dass man sich auf die Suche nach einem Rechtfertigungsgrund machen müsste, die in den meisten Fällen auch eher fruchtlos bleiben wird. Notwehr kommt als Rechtfertigung nicht in Betracht.[51] Es fehlt an einem gegenwärtigen Angriff, denn Honeypots sollen nur zukünftige Angriffe verhindern.[52] Als antizipierte Nothilfe können die Pots nicht erfasst werden, da sie zunächst den Angriff nicht verhindern, sondern sie gerade ermöglichen. Sie sind daher kein geeignetes Mittel, um einen konkreten Angriff abzuwenden.[53] Auch ein rechtfertigender Notstand scheidet aus demselben Grund aus.[54] Ebenso wenig können sich der Rechtfertigungsgrund der Einwilligung bzw. das Einverständnis zu Gunsten der IT-Forschenden auswirken. Zu Recht wird darauf hingewiesen, dass die IT-Forschenden im Vorfeld des Angriffs keine Kenntnisse über die Person der Angegriffenen verfügen; erst nach dem Starten des Angriffs können sie Kenntnisse über die Angriffsrichtung erlangen, für das Einholen der Einwilligung ist es dann zu spät.[55] Zur Frage einer mutmaßlichen Einwilligung wird zutreffend angemerkt, man solle in Anbetracht der schwerwiegenden wirtschaftlichen Folgen einer D[R]DoS-Attacke für das Opfer nicht vorschnell von einer solchen ausgehen.[56] Vor diesem Hintergrund wird das Heranziehen der Wissenschaftsfreiheit[57] gem. Art. 5 Abs. 3 Alt. 2 GG als allgemeiner Rechtfertigungsgrund oder die Rechtfertigung über den Gedanken der Ausübung einer beruflichen Pflicht diskutiert,[58] die rechtliche Lage bleibt allerdings letztlich einstweilen ungeklärt. Daher auch die Aufforderung an den Gesetzgeber, durch die Einführung eines expliziten Rechtfertigungsgrunds für IT-Forschende die Rechtsunsicherheiten zu beseitigen.[59]

Zweifellos wäre das Tätigwerden des Gesetzgebers die optimale Lösung, um das Feld erlaubter IT-Forschung genau zu bestimmen und Rechtsunsicherheiten auszuräumen. Bis dahin ist es jedoch schon jetzt möglich, eine Leitlinie zu entwerfen, die dabei helfen kann, strafwürdige von nicht-strafwürdiger Forschung zu unterscheiden.

---

47 *Roxin*, Strafrecht AT, Bd. 2, 2003, § 26 Rn. 271.
48 Statt vieler *Rengier*, Strafrecht AT, § 45 Rn. 65 ff.
49 *Rengier*, Strafrecht AT, § 45 Rn. 65.
50 Vgl. *Sommer*, JR 1986, 485.
51 *Vogelgesang/Möllers/Potel*, MMR 2017, 291 (293 f.); *Wörner/Blocher* (Fn. 4), S. 76.
52 *Vogelgesang/Möllers/Potel*, MMR 2017, 291 (293 f.); *Wörner/Blocher* (Fn. 4), S. 76. Man muss hier nicht unbedingt die Gegenwärtigkeit ablehnen. Man könnte überlegen, die Gegenwärtigkeit der Gefahr in Form der Dauergefahr zu bejahen. Dies wird auch in Bezug auf ohne Beauftragung durchgeführte proaktive Sicherheitstests zur Aufdeckung von Sicherheitslücken („Penetrationstests") angenommen, die später von Cyberkriminellen ausgenutzt werden. Die Dauergefahr („Ticking-Time-Bomb-Situationen") wird aufgrund der vorhandenen Sicherheitslücken bejaht, die jederzeit entdeckt und ausgenutzt werden können, *Bao/Zech*, in: Golla/Brodowski, IT-Sicherheitsforschung und IT-Strafrecht, 2023, S. 131 (145). Solche Sicherheitsdefizite sollen auch durch den Einsatz von Honeypots identifiziert werden. Allerdings müsste man, anders bei dem Fall der proaktiven Sicherheitstests, die Geeignetheit der Verwendung von Honeypots zur Gefahrabwehr ablehnen, vgl. *Wörner/Blocher* (Fn. 4), S. 76. Aber auch die Rechtfertigung der Durchführung von „Penetrationstests" nach § 34 StGB wird am Ende doch nicht einfach zu bejahen sein, spätestens bei der Stufe der Interessenabwägung entstehen Schwierigkeiten, dazu *Bao/Zech* (Fn. 56), S. 131 (145 f.).
53 *Vogelgesang/Möllers/Potel*, MMR 2017, 291 (293 f.); *Wörner/Blocher* (Fn. 4), S. 76.
54 *Wörner/Blocher* (Fn. 4), S. 76.
55 *Vogelgesang/Möllers/Potel*, MMR 2017, 291 (293); *Wörner/Blocher* (Fn. 4), S. 76.
56 *Wörner/Blocher* (Fn. 4), S. 76.
57 Zum allgemeinen Verhältnis von Wissensfreiheit und strafrechtlicher Sanktionierung s. *Krüger/Sorge/Vogelgesang* (Fn. 39), S. 529 (532); vgl. dazu auch *Nestler*, GA 2023, 566 (567 f.)
58 *Vogelgesang/Möllers/Potel*, MMR 2017, 291 (294); *Wörner/Blocher* (Fn. 4), S. 78 ff.
59 *Wörner/Blocher* (Fn. 4), S. 79.

Dies lässt sich, wie oben erwähnt, bereits auf der Tatbestandsebene durch Bestimmung des sog. Vollendungsvorsatzes des Teilnehmers erreichen. Bereits mit Blick auf die Lockspitzel-Fälle herrscht die Ansicht vor, dass die Vollendung als Bezugsgröße des Teilnehmervorsatzes nicht mit der formellen Tatbestandserfüllung gleichzusetzen ist. Von dieser Grundannahme ausgehend wird der „Eintritt des materiellen Vollendungs-Erfolgs“[60] verlangt, der in der Herbeiführung der eigentlichen Rechtsgutsverletzung oder in der Entstehung eines irreparablen Schadens gesehen wird.[61] Die Rechtsgutsverletzung benötigt aufgrund des häufig abstrakten Gehalts des Rechtsgutes eine Konkretisierung durch das Erfolgsunrecht, das die jeweilige Strafnorm erfassen will.[62] Man fragt also, welchen sozialschädlichen Sachverhalt die konkrete Norm verhindern will und ob der Teilnehmer diesen Sachverhalt in seinen Vorsatz aufgenommen hat.[63] Am Beispiel des „Handeltreibens“ in § 29 Abs. 1 Nr. 1 BtMG lässt sich die Problematik veranschaulichen. Durch § 29 BtMG soll vermieden werden, dass ein Rauschgift in den unkontrollierten Umlauf kommt. Ein Agent provocateur, der einen Dealer veranlasst, Drogen zu kaufen, und dabei Sicherungsvorkehrungen und Kontrollmaßnahmen trifft, dass nach der Übergabe kein Umsatz gemacht wird, schafft nicht die Situation, die § 29 BtMG verhindern will.[64] Der Veranlasser sorgt vielmehr dafür, dass das Rauschgift nicht auf dem Markt kommt.[65] Kontroll-und Sicherheitsvorkehrungen funktionieren als „Tatbestandskorrektiv“.[66]

Ähnlich wird bei sog. Tatbeständen mit rechtsgutbezogenen Absichtsmerkmalen argumentiert, etwa bei § 146 Abs. 1 Nr. 1 StGB, wonach Täter ist, wer Geld in der Absicht nachmacht, dass es als echt in Verkehr gebracht oder dass ein solches Inverkehrbringen ermöglicht werde, oder Geld in dieser Absicht so verfälscht, dass der Anschein eines höheren Wertes hervorgerufen wird. Der Anstifter selbst muss diese rechtsgutbezogenen Absichten nicht haben, es genügt, wenn er weiß und will, dass der Täter die Absicht, hier etwa die Absicht, das falsche Geld in Verkehr zu bringen, verwirklichen kann.[67] Lässt der Agent provocateur, der vorher den Täter zu einer Falschmünzerei veranlasst hat, durch das Treffen von Interventionsvorkehrungen nicht zu, dass das Falschgeld in den Umlauf gelangt, ist er wegen fehlenden Vollendungsvorsatzes straffrei.[68]

3. Fehlender Vollendungsvorsatz bei „Interventions- bzw. Wiedergutmachungswillen“

Wenden wir uns nun vor diesem Hintergrund dem Problem um die Strafbarkeit des Honeypots-Betreibers zu. An erster Stelle kommt eine Beihilfe zur Computersabotage nach § 303b StGB in Betracht. Schutzgut der Norm ist das Interesse der Betreiber und Nutzer eines Datenverarbeitungssystems an einem störungsfreien und ordnungsgemäßen Ablauf der Datenverarbeitung.[69] Der sozialwidrige Sachverhalt, den die Norm daher verhindern will, ist die Verursachung von nachteiligen Störungen, unter anderem durch gezielte Überlastung von Internetverbindungen. § 303b StGB ist außerdem ein Tatbestand mit einem rechtsgutbezogenen Absichtsmerkmal, nämlich der Nachteilszufügungsabsicht. Würde man das Kriterium des „materiellen Vollendungserfolgs“ bzw. der Rechtgutsverletzung unmittelbar auf den Fall von Honeypot-Betreibern übertragen, müsste man zwangsläufig stets zu dem Ergebnis kommen, dass die IT-Forschenden sich wegen Beihilfe zu § 303b StGB strafbar machen. Faktisch werden sie oft nicht die Möglichkeit einer rechtzeitigen Intervention vor der vollständigen Durchführung des D[R]DoS-Angriffs haben, um die Realisierung des von § 303b StGB erfassten sozialschädlichen Sachverhalts zu verhindern, was ihnen auch bewusst sein wird. Anders als im Fall des Handeltreibens nach § 29 BtMG können Angriffe und Rechtsgutverletzungen im digitalen Raum in Bruchteilen von Sekunden erfolgen. Man müsste dann stets einen Vollendungsvorsatz bejahen. Dies ist allerdings angesichts der typischerweise kurzen Versuchsphase eines digitalen Angriffs bedenklich.

Digitale Vorgänge sollten nicht nach den gleichen Zeitmaßstäben wie analoge behandelt werden und Kontrollmöglichkeiten im digitalen Raum sollten nicht mit analogen Kontrollmöglichkeiten gleichgesetzt werden. Die sich aus den faktischen Gegebenheiten digitaler Abläufe ergebende zeitliche Vorverlagerung der Vollendung im Vergleich zu herkömmlichen analogen Delikten ist bei der Bestimmung des Vollendungsvorsatzes einzubeziehen. Man kann den Gedanken der tätigen Reue aufgreifen und in den Vollendungsvorsatz des Honeypot-Betreibers integrieren. Will der IT-Forschende gleich nach der Durchführung des Angriffs mit einem „Wiedergutmachungsvorsatz“ intervenieren, worunter auch die Identifizierung des beobachteten Täters fällt, und trifft er entsprechende Sicherheitsvorkehrungen und Kontrollmaßnahmen, ist sein Vorsatz nicht auf die Vollendung der Haupttat gerichtet. Man kann hier eine Parallele zu *Günter Jakobs'* Beispiel eines straffreien Agent provocateurs ziehen, der sein „Rücktrittverhalten“ im Vorfeld plant: „[Straffrei ist] der Anstifter zur Brandstiftung [, der] eine sicher wirkende automatische Löschungseinrichtung installiert oder [bereit steht], den Brand gewiß sofort zu löschen.“[70] Trotz der Vollendung der Tat fehlt dem Anstifter hier der Vollendungsvorsatz. Ähnlich verhält es sich mit einem zur Intervention bereitstehenden Honeypot-Betreiber. Eine Beihilfe zur Computersabotage scheidet in einem solchen Fall aus. Aus demselben Grund kann auch eine Strafbarkeit nach §§ 303a, 27 StGB abgelehnt werden.

---

60 *Fischer*, StGB, § 27 Rn. 27.
61 Dazu *Sommer*, JR 1986, 485 (486).
62 Dazu *Sommer*, JR 1986, 485 (488 f.); vgl. *Jakobs*, Strafrecht AT, Part 2, 1991, 23. Abschn. Rn. 17.
63 *Sommer*, JR 1986, 485 (488 ff).; vgl. *Roxin*, Strafrecht AT, Bd. 2, § 26 Rn. 157.
64 *Roxin*, Strafrecht AT, Bd. 2, § 26 Rn. 157; *Sommer*, JR 1986, 485 (491); *Schwarzburg*, NStZ 1995, 469 (470 f.); vgl. auch *Jakobs*, Strafrecht AT, Part 2, 23. Abschn. Rn. 17.
65 *Roxin*, Strafrecht AT, Bd. 2, § 26 Rn. 157.
66 *Schwarzburg*, NStZ 1995, 469 (470).
67 *Roxin*, Strafrecht AT, Bd. 2, § 26 Rn. 164.
68 *Roxin*, Strafrecht AT, Bd. 2, § 26 Rn. 164.
69 *Hilgendorf*, in: SSW-StGB, § 303b Rn. 10; s. auch *Hilgendorf/Kusche/Valerius*, Computer- und Internetstrafrecht, Rn. 423.
70 *Jakobs*, Strafrecht AT, Part 2, 23. Abschn. Rn. 17.

D[R]DoS-Angriffe werden oft mit Erpressungsabsicht durchgeführt. Daher ist auch zu diskutieren, ob eine Beihilfe zur Erpressung nach §§ 253, 27 StGB gegeben ist. Zum Teil wird dies mit der Begründung abgelehnt, dass der Gehilfe nicht unbedingt wissen müsse, dass es sich bei der Tat um eine Erpressung handelt.[71] Da die Besonderheiten des Einzelfalls den IT-Forschenden in der Regel nicht bekannt seien, könne sich ihr Vorsatz insoweit auch nicht auf die Erpressung als Haupttat beziehen.[72] Zwar ist diese Auffassung im Ergebnis richtig, die Begründung überzeugt allerdings nicht. Wie schon oben erwähnt, sind die Anforderungen an den Gehilfenvorsatz gering. „Beihilfe durch Tat kann […] schon begehen, wer dem Täter ein entscheidendes Tatmittel willentlich an die Hand gibt und damit bewusst das Risiko erhöht, dass eine durch den Einsatz gerade dieses Mittels typischerweise geförderte Haupttat verübt wird“ hebt der *BGH* hervor.[73] Dass durch Honeypots ermöglichte D[R]DoS-Angriffe typischerweise zur Begehung von Erpressungen erfolgen, dürfte IT-Forschenden bekannt sein.[74] Es dürfte ihnen also bewusst sein, dass durch das Betreiben des Honeypots das Risiko erhöht wird, dass Erpressungen verübt werden. Die Überzeugungskraft des Arguments, der Vorsatz beziehe sich nicht auf die Haupttat, ist deswegen zweifelhaft. Will man gleichwohl den Gehilfenvorsatz richtigerweise ablehnen, sollte man seine Aufmerksamkeit wieder auf die Vollendung der Haupttat richten.

Bei der Erpressung handelt es sich um einen Tatbestand mit einer nicht rechtsgutsbezogen Absicht, nämlich einer Bereicherungsabsicht. Die Behandlung des Vollendungsvorsatzes im Zusammenhang mit solchen Tatbeständen ist umstritten. Nach einer Auffassung muss jeder Beteiligte die Verwirklichung der Bereicherungsabsicht wollen, wenn nicht, scheidet ein Vollendungsvorsatz aus.[75] Nach einer zweiten Ansicht liegt Vollendungsvorsatz hingegen auch dann vor, wenn der Beteiligte die Bereicherung des Täters oder eines Dritten nicht will, sofern er die Vermögensschädigung in seinen Vorsatz aufgenommen hat[76]: „Wenn jemand einen anderen zum Betrug auffordert und dabei die Vermögensschädigung des Opfers, nicht aber die Bereicherung des Täters oder eines Dritten von seinem Vorsatz umfaßt ist […], liegt beim Veranlasser ein Rechtsgutangriff vor; denn er will den Betroffenen an seinem Vermögen schädigen. Das muß für eine Anstiftung ausreichen; denn die Bereicherungsabsicht ist nicht für die Strafwürdigkeit des Anstifters, sondern nur für den Deliktstyp […] wichtig.“[77] Auf dem Boden beider Auffassungen kann der Vollendungsvorsatz der IT-Forschenden verneint werden. Voraussetzung dafür ist, dass der Wille vorhanden ist, die materielle Beendigung zu verhindern. Ein auf Vermögensschädigung, geschweige denn auf eine Bereicherung des Täters oder eines Dritten gerichteter Vorsatz wird nicht vorliegen, sofern der Wille der IT-Forschenden (genau wie der Wille des agent provocateurs bei Diebesfallen) darauf gerichtet ist, durch rechtzeitiges Eingreifen einen dauerhaften Vermögensschaden zu verhindern. Dieser Wille manifestiert sich darin, dass im Vorfeld des Angriffs bereits Kontrollmaßnahmen und Vorkehrungen zur Identifizierung des späteren Täters sowie zur Neutralisierung des bisherigen technischen Beitrags zum D[R]DoS-Angriff getroffen sind.

III. Fazit

Zusammenfassend lässt sich feststellen: Es ist umstritten, ob das Betreiben von Honeypots zum Zweck der IT-Forschung Strafbarkeitsrisiken mit sich bringt. Während nach einigen Stimmen eine Beihilfe zu den Straftaten Dritter in Betracht kommt – man versucht dann einen Ausweg aus der Strafbarkeit auf der Rechtfertigungsebene zu finden –, lehnt eine andere Ansicht wegen fehlenden Schädigungszwecks bereits den Beihilfevorsatz ab. Gezeigt wurde, dass die zweite Ansicht überzeugender ist, da die ferneren bzw. mittelbaren Bestrebungen der IT-Forschenden bezüglich der Verbesserung von IT-Sicherheitssystemen bei der Frage des Vorsatzes einbezogen werden. Dieser im Prinzip richtige Ansatz bedarf allerdings einer genaueren dogmatischen Untermauerung. Dafür steht die ausdifferenzierte Dogmatik zum Vollendungsvorsatz im Zusammenhang mit den Lockspitzel-Fällen zur Verfügung. Argumentiert wurde, dass die im Rahmen dieser Diskussion entwickelten Leitlinien zur Bestimmung des Vollendungsvorsatzes zwar auf die Frage des Gehilfenvorsatzes der IT-Forschenden übertragbar sind, jedoch nicht ohne an die Besonderheiten digitaler Abläufe angepasst zu werden. Zu beachten ist daher, dass es bei digitalen Vorgängen aufgrund der technischen Gegebenheiten oft zu einer zeitlichen Vorverlagerung der Vollendung im Vergleich zu herkömmlichen analogen Delikten kommt – ein Angriff kann in manchen Fällen schon durch einige wenige Mausklicks ausgelöst werden. Für die Problematik der Strafbarkeit von Honeypot-Betreibern bedeutet dies, dass großzügigere Maßstäbe bei der Bestimmung des Vollendungsvorsatzes zugrunde zu legen sind als bei analogen Vorgängen. Will der IT-Forschende gleich nach der Durchführung des Angriffs mit einem „Wiedergutmachungswillen“ intervenieren und trifft er oder sie entsprechende Kontrollmaßnahmen, ist trotz formeller Vollendung der Tat sein Vorsatz nicht auf die Vollendung der Haupttat gerichtet. Eine Beihilfestrafbarkeit scheidet daher aus.

---

71 *Vogelgesang/Möllers/Potel*, MMR 2017, 291 (294).
72 *Vogelgesang/Möllers/Potel*, MMR 2017, 291 (294).
73 BGHSt 42, 135 (138).
74 Es geht hier nicht allein um die Kenntnis eines generellen Risikos der Tatförderung, dazu *Fischer*, StGB, § 27 Rn. 26.
75 *Jakobs*, Strafrecht AT, Part 2, 23. Abschn. Rn. 20.
76 *Roxin*, Strafrecht AT, Bd. 2, § 26 Rn. 166.
77 *Roxin*, Strafrecht AT, Bd. 2, § 26 Rn. 166.