„Mittelbare Täterschaft“ durch kompromittierte Systeme
Grenzen personenbezogener Zurechnung im digitalen Raum

von RA Dr. Dr. Fabian Teichmann, LL.M. (London), EMBA (Oxford)[*]

Abstract
Digitale Angriffe werden häufig nicht durch einen menschlichen Tatmittler, sondern über kompromittierte Endgeräte, Botnetze und automatisierte Skripte ausgeführt. Dogmatisch liegt deshalb nahe, die Figur der mittelbaren Täterschaft gemäß § 25 Abs. 1 Alt. 2 StGB als Zurechnungsinstrument zu bemühen: Der Hintermann handelt „durch“ infizierte Systeme, ohne selbst am Zielsystem präsent zu sein. Der Beitrag zeigt jedoch, dass eine solche Ausweitung die personenbezogene Struktur der mittelbaren Täterschaft verfehlt. § 25 Abs. 1 Alt. 2 StGB setzt einen Tatmittler als Person voraus. Nicht-personale Durchführungsmittel sind, dogmatisch präzise, Werkzeuge der unmittelbaren Täterschaft. Im digitalen Raum ist daher zwischen Werkzeuggebrauch (unmittelbare Täterschaft), objektiver Zurechnung automatisierter Erfolgsverläufe und echten Konstellationen mittelbarer Täterschaft über menschliche Intermediäre (etwa bei Social Engineering, Irrtums- oder Zwangslagen) zu differenzieren. Nur wo organisationsbezogene Rahmenbedingungen regelhafte, vom Hintermann beherrschte Abläufe auslösen, kann – jenseits klassischer Defektlagen – ein Rückgriff auf Organisationsherrschaft in Betracht kommen. Die vorgeschlagenen Kriterien werden anhand der Delikte der Datenveränderung gemäß § 303a StGB[1] und Computersabotage gemäß § 303b StGB[2] sowie typischer Botnet[3]- und Ransomware-Abläufe[4] dargestellt. Kriminalpolitisch folgt daraus, dass einer Ausweitung des § 25 Abs. 1 Alt. 2 StGB auf technische Durchführungsmittel nicht nur dogmatische, sondern auch rechtsstaatliche Bedenken entgegenstehen: Eine solche Ausdehnung würde das Bestimmtheitsgebot (Art. 103 Abs. 2 GG) strapazieren und die ordnende Funktion des Beteiligungssystems schwächen. Zugleich zeigt die Untersuchung, dass der Gesetzgeber mit den bestehenden Instrumenten - unmittelbare Täterschaft, Vorbereitungstatbestände und objektive Zurechnung - über ein hinreichendes und ausdifferenziertes Regelungsarsenal verfügt, das einer unkontrollierten Vorverlagerung der Täterstrafbarkeit nicht bedarf.

Digital attacks are frequently carried out not by a human intermediary but through compromised end devices, botnets, and automated scripts. From a doctrinal perspective, this raises the question of whether the concept of indirect perpetration (mittelbare Täterschaft) under § 25(1) alternative 2 of the German Criminal Code (StGB) can serve as a basis for attribution: the principal acts "through" infected systems without being physically present at the target. This article demonstrates, however, that such an extension would misconceive the person-based structure of indirect perpetration. Section 25(1) alternative 2 presupposes an intermediary who is a person. Non-personal means of execution are, in doctrinally precise terms, tools of direct perpetration (unmittelbare Täterschaft). In the digital context, it is therefore necessary to distinguish between the use of tools (direct perpetration under § 25(1) alternative 1), the objective attribution (objektive Zurechnung) of automated causal processes, and genuine instances of indirect perpetration through human intermediaries, in particular in cases of social engineering, mistake, or coercion. Only where organisational frameworks produce regular, principal-controlled sequences of conduct can organisational control (Organisationsherrschaft) - itself a contested doctrine - be considered, and even then only with respect to human organisational structures, not technical systems. The proposed criteria are illustrated by reference to the offences of data manipulation (§ 303a StGB), computer sabotage (§ 303b StGB), and typical botnet and ransomware attack scenarios. From a criminal policy perspective, the analysis demonstrates that an extension of § 25(1) alternative 2 to technical means of execution would not only strain the principle of legal certainty (Bestimmtheitsgebot, Article 103(2) of the Basic Law) but would also undermine the ordering function of the participation system. The legislature has already provided targeted instruments for the anticipatory criminalisation of preparatory conduct in the digital sphere (§§ 202c, 303a(3), 303b(5) StGB). There is accordingly no criminal policy need to expand the concept of perpetration; the existing doctrinal framework - direct

[*] *RA Dr. Dr. Fabian Teichmann, LL.M. (London), EMBA (Oxford)* ist Lehrbeauftragter an der Universität zu Köln, der Universität Kassel und der Universität Trier sowie Managing Partner der Teichmann International (Schweiz) AG.

[1] *Hecker*, in: TK-StGB, 31. Aufl. (2025), § 303a Rn. 4–8; *Bär*, in: Handbuch des Wirtschaftsstrafrechts, 6. Aufl. (2025), 15. Kap. Rn. 114–118; *Altenhain*, in: Matt/Renzikowski, StGB, 2. Aufl. (2020), § 303a Rn. 6–10; *Wengenroth*, in: Handbuch der Datenschutzsanktionen, 2023, § 21 Rn. 17.

[2] *Mahn*, in: Wirtschaftsstrafrecht, 3. Aufl. (2023), Kap. 11 Rn. 196, 197; *Hecker*, in: TK-StGB, 31. Aufl. (2025), § 303b Rn. 5-8; *Wieck-Noodt*, in: MüKo-StGB, 4. Aufl. (2022), § 303b Rn. 10; *Mansdörfer*, in: BeckOK IT-Recht, 20. Ed. (1.7.2025), § 303b Rn. 10–21.

[3] BSI, Botnetze, Auswirkungen und Schutzmaßnahmen, abrufbar unter: http://bit.ly/4bmLdKE (zuletzt abgerufen am 29.1.2026); *Schmidt/Pruß*, in: Auer-Reinsdorff/Conrad, IT- und Datenschutzrecht, 3. Aufl. (2019), § 3 Rn. 270; *Maihold*, in: Bankrechts-Handbuch, 6. Aufl. (2022), § 33 Rn. 64, 6; *Graf*, in: MüKo-StGB, 5. Aufl. (2025), § 202a Rn. 8.

[4] Polizeiliche Kriminalprävention, Ransomware ist Tor zur digitalen Erpressung, abrufbar unter: https://bit.ly/4r7wRCo (zuletzt abgerufen am 29.1.2026); BSI, Ransomware – Fakten und Abwehrstrategien, abrufbar unter: https://bit.ly/3P0i7YN (zuletzt abgerufen am 29.1.2026); *Spiecker gen. Döhmann/Bretthauer*, Dokumentation zum Datenschutz, 2025, Rn. 16; *Sohr/Kemmerich*, in: Kipker, Cybersecurity-Handbuch, 2. Aufl. (2023), Kap. 3 Rn. 177.

perpetration through the use of tools, objective attribution, and delict-specific preparatory offences - is sufficient to capture digital attack scenarios comprehensively and with the precision that the rule of law demands.

I. Problemstellung und Gang der Untersuchung

Angriffe auf informationstechnische Systeme sind heute regelmäßig arbeitsteilig, skalierbar und technisch vermittelt organisiert. Typische Modelle –Botnet-Betrieb, Ransomware-as-a-Service, DDoS-Erpressung – zeichnen sich dadurch aus, dass der eigentliche Eingriff am Zielsystem nicht als körperliche Handlung des Angreifers erscheint, sondern als Systemreaktion: Pakete werden automatisiert versandt, Befehle als „Command-and-Control"-Nachrichten verteilt, Skripte ohne weitere menschliche Zwischenschritte ausgeführt. Der Angreifer ist räumlich abwesend; die Ausführung „passiert" an vielen Orten zugleich.[5]

Diese Struktur verschiebt den dogmatischen Fokus. Während im klassischen Deliktsbild das Tatgeschehen an eine menschliche Ausführungshandlung am Tatort anknüpft, treten im digitalen Raum Fernsteuerung, Automatisierung und Delegation an technische Mittel in den Vordergrund. Für die Zurechnung stellt sich daher wiederkehrend die Frage, ob das Strafrecht eine personelle Vermittlung voraussetzt oder ob technische Durchführungsmittel als „Tatmittler" im Sinne der Beteiligungsdogmatik verstanden werden können.

Das Problem konzentriert sich auf § 25 Abs. 1 Alt. 2 StGB. Mittelbare Täterschaft ist das klassische Instrument, um Tatbegehung „über Dritte" zu erfassen.[6] Der Hintermann beherrscht den Tatablauf, weil er einen anderen als Werkzeug einsetzt.[7] Im digitalen Raum scheint diese Figur auf den ersten Blick anschlussfähig: Der Täter bedient sich kompromittierter Systeme[8] und lässt sie „für sich" handeln. Zugleich fehlt in den typischen Fällen jeder menschliche Tatmittler als Defizitträger. § 25 Abs. 1 Alt. 2 StGB beschreibt aber "durch einen anderen begeht", womit ein Mensch gemeint ist, auch wenn dieser als Werkzeug verwendet wird.[9] Die Systeme sind aber keine Personen; sie können weder irren noch vorsätzlich handeln. Die Leitfrage lautet deshalb: Kann (und soll) § 25 Abs. 1 Alt. 2 StGB dort tragen, wo der Täter über Botnetze oder autonome Skripte agiert, obwohl kein menschlicher Tatmittler vorliegt?

Die Antwort ist nicht bloß terminologisch. Eine, auch nur stillschweigende, „Digitalisierung" der mittelbaren Täterschaft hätte Folgewirkungen für die Abgrenzung zu unmittelbarer Täterschaft, Versuch und Rücktritt sowie für die Anschlussfähigkeit organisationsbezogener Herrschaftsmodelle. Zugleich würde sie die dogmatische Begrenzungsfunktion des Beteiligungssystems schwächen. Wo technische Wichtigkeit genügt, droht eine Zurechnungsentgrenzung, die das Tatbestandsprinzip und die Differenzierung zwischen Täterschaft und Teilnahme verwässert.

Der Beitrag folgt daher einem dreistufigen Programm, bei dem zunächst Struktur und Begrenzungsfunktion der mittelbaren Täterschaft als personenbezogene Zurechnungsfigur herausgearbeitet werden (II). Sodann wird geprüft, ob und mit welchen Argumenten Botnetze und Skripte als „Tatmittler" verstanden werden könnten – und warum dies dogmatisch nicht trägt (III). Abschließend werden Alternativmodelle entwickelt, die digitale Angriffe ohne dogmatische Verwerfungen erfassen: unmittelbare Täterschaft durch Werkzeuggebrauch, objektive Zurechnung automatisierter Verläufe sowie – in engen Grenzen – Organisationsherrschaft und echte mittelbare Täterschaft über menschliche Intermediäre (IV/V).

Die Fragestellung hat dabei nicht nur dogmatische, sondern auch kriminalpolitische Tragweite. Der zunehmende Verfolgungsdruck im Bereich der Cyberkriminalität begünstigt die Versuchung, über expansive Zurechnungskonstruktionen - etwa die Gleichsetzung technischer Systeme mit Tatmittlern - Beweisschwierigkeiten dogmatisch zu kompensieren. Demgegenüber steht das rechtsstaatliche Gebot, die Grenzen des Beteiligungssystems nicht aus kriminalpolitischer Opportunität zu verschieben. Die nachfolgende Untersuchung versteht sich daher auch als Beitrag zur kriminalpolitischen Debatte um die Reichweite und Begrenzung strafrechtlicher Zurechnungsfiguren im digitalen Raum.

II. Personenbezogenheit der mittelbaren Täterschaft: Funktion, Struktur und Tatmittlerdefizit

1. Ausgangspunkt ist der Gesetzestext

§ 25 StGB unterscheidet drei Grundformen der Täterschaft: unmittelbare Täterschaft („wer die Tat selbst

---

5 IDW, Cyberrisk, Ziff. 2, abrufbar unter: https://bit.ly/4r9RM7Y (zuletzt abgerufen am 29.1.2026); LDI, Hilfe, ein Cyberangriff, abrufbar unter: https://www.ldi.nrw.de/cyberangriff (zuletzt abgerufen am 29.1.2026); *Lapp* in: Kipker Cybersecurity-HdB, 2. Aufl. (2023), Kap. 10 Rn. 140, 141; *Marly/Hessel,* Softwarerecht, 8. Aufl. (2024), § 14 Rn. 6–8; *Schildbach/Groothuis,* DSRI Herbstakademie 2025, 2025; *Teichmann,* Polizei 2025, 401; *Teichmann*, NZI 2025, 809.

6 *Haas,* in: Matt/Renzikowski, StGB, § 25 Rn. 5-7; *Pohlreich,* in: Lackner/Kühl/Heger, StGB, 31. Aufl. (2025), § 25 Rn. 2; *Weißer,* in: TK-StGB, 31. Aufl. (2025), § 25 Rn. 3, 4; *Kindhäuser/Hilgendorf,* LPK-StGB, 10. Aufl. (2025), § 25 Rn. 7-8; *Kudlich*, in: BeckOK-StGB, 67. Ed. (1.11.2025), § 25 Rn. 19; *Scheinfeld*, in: MüKo-StGB, 5. Aufl. (2024), § 25 Rn. 60-62.

7 *Ingelfinger*, in: Dölling/Duttge/Rössner, StGB, 5. Aufl. (2022), § 25 Rn. 17–20; *Schild/Kretschmer*, in: NK-StGB, 6. Aufl. (2023), § 25 Rn. 26–28; *Scheinfeld,* in: MüKo-StGB, § 25 Rn. 61-64; *Rübenstahl*, in: Böttger, Wirtschaftsstrafrecht, 3. Aufl. (2023), Kap. 18 Rn. 31–35.

8 IT-Business, Definition: Was ist kompromittieren, abrufbar unter: https://bit.ly/3OXEP3K (zuletzt abgerufen am 29.1.2026); BSI, Prävention und Erste Hilfe bei Webseiten Kompromittierung oder Defacement, Ziff. 2, abrufbar unter: https://bit.ly/3Ni3nnF (zuletzt abgerufen am 29.1.2026).

9 *Schild/Kretschmer,* in: NK-StGB, § 25 Rn. 73-79; *Weißer*, in: TK-StGB, § 25 Rn. 5; *Kudlich*, in: BeckOK-StGB, § 25 Rn. 20.

begeht“, Abs. 1 Alt. 1)[10], mittelbare Täterschaft („wer die Tat … durch einen anderen begeht“, Abs. 1 Alt. 2)[11] und Mittäterschaft (Abs. 2)[12]. Der Wortlaut „durch einen anderen“ ist dabei nicht austauschbar. Er meint nach verbreiteter Auffassung einen „anderen“ als Person: „Begehen ‚durch einen anderen‘ bedeutet eines Menschen, also dem Ausführungstäter.[13]

Damit ist die mittelbare Täterschaft begrifflich als personale Vermittlung konstruiert. Das ist dogmatisch plausibel, weil § 25 Abs. 1 Alt. 2 StGB nicht (nur) eine Kausalitätsfigur ist, sondern eine Verantwortungsfigur. Der Hintermann wird Täter, obwohl er die tatbestandliche Handlung nicht selbst ausführt, weil ihm die Ausführungshandlung des Tatmittlers zugerechnet wird.[14] Zurechnungsgrund ist die Herrschaft über einen defizitären oder strukturell unterlegenen Mittler. Der Hintermann „steht“ im Zentrum, weil er die entscheidende Disposition über das Ob und Wie der Tatbestandsverwirklichung innehat – und zwar mittels einer anderen Person.

2. Das Tatmittlerdefizit ist der Kern

Klassische Fallgruppen beruhen darauf, dass der Mittler entweder (i) ohne Vorsatz handelt (Irrtum), (ii) schuldunfähig oder entschuldigt ist, (iii) unter Zwang steht oder (iv) aufgrund normativer Defizite nicht als Täter erfasst wird wie z.B. fehlende Sonderpflichten oder Absichten. In all diesen Konstellationen ist entscheidend, dass der Mittler als Person handelt und sein Handeln (oder Unterlassen) tatbestandsrelevant ist.[15]

3. Historische und systematische Einbettung

Die Personenbezogenheit ist auch vor dem Hintergrund der Täterschaftstheorien zu verstehen. Das Gesetz spricht nicht von Tatherrschaft, sondern formuliert die Täterschaftsformen offen. Die dogmatische Debatte über formal-objektive Theorie, subjektive Theorie, Tatherrschaftslehre und Einheitstäterschaft ist dadurch nicht obsolet, sondern in die Aufgabe übersetzt, die in § 25 StGB angelegten Formen mit trennscharfen Kriterien zu füllen. Die Vorbemerkungen zu § 25 StGB zeichnen nach, dass das Kriterium der Tatherrschaft in der Lehre dominiert und in der Rechtsprechung jedenfalls als Indiz im Rahmen einer Gesamtwürdigung anerkannt ist, während zugleich betont wird, dass im Gesetz von Tatherrschaft nicht die Rede ist und „Zentralgestalt“ ohne Konkretisierung inhaltsleer bleibt.[16] Diese Einbettung ist für digitale Konstellationen bedeutsam, weil sie zeigt, dass „Herrschaft“ nicht mit „Techniknähe“ gleichgesetzt werden darf. Die Gefahr einer dogmatischen Abkürzung ist im Digitalen besonders hoch, denn wer die Infrastruktur kontrolliert, wirkt faktisch zentral; daraus folgt aber nicht automatisch, dass die Tat „durch einen anderen“ begangen wird. Die Formenlehre verlangt eine normative Zurechnungsentscheidung, die an den gesetzlichen Formen festhält.

4. Begrenzungsfunktion

Die Personenbezogenheit verhindert, dass § 25 Abs. 1 Alt. 2 StGB zur bloßen Formel für Fernwirkung oder technisches „Outsourcing“ wird. Wäre jede mittelbare Erfolgsherbeiführung zugleich „Begehen durch einen anderen“, verlöre die Abgrenzung zu § 25 Abs. 1 Alt. 1 StGB ihre Konturen; Alt. 2 würde die Werkzeugkategorie absorbieren. Die Beteiligungsformenlehre würde damit ihre ordnende und begrenzende Funktion einbüßen.

5. Der digitale Kontext als Stresstest

Technische Beiträge sind oft hochwirksam, ohne dass daraus eine personale Herrschaftsrelation folgt. Ein Bot „führt“ Befehle aus, aber er „entscheidet“ nicht;[17] er unterliegt keinem Irrtum und keinem Zwang; er ist kein Normadressat. Die Zurechnungsfrage ist daher nicht, ob ein Defekt vorliegt, sondern ob der Täter einen tatbestandsspezifischen Gefahrenverlauf in Gang gesetzt hat, der sich im Erfolg realisiert.

6. Der Grenzfall

„Tatmittler gegen sich selbst“. Wenn ein Täter eine Falle stellt und das Opfer durch eigenes Verhalten, etwa das Öffnen einer präparierten Sendung, den Erfolg auslöst, wird das Opfer bisweilen als Tatmittler verstanden.[18] Der Streit dreht sich dann um Versuchsbeginn und die Frage, wann der Täter „angesetzt“ hat.[19] Der Tatmittler bleibt aber eine Person; die Diskussion setzt ein voluntatives

---

10 *Weißer,* in: TK-StGB, § 25 Rn. 2; *Haas,* in: Matt/Renzikowski, StGB, § 25 Rn. 2-4; *Kudlich,* in: BeckOK-StGB, § 25 Rn. 18, 18.1; *Pohlreich,* in: Lackner/Kühl/Heger, StGB, § 25 Rn. 1-1a; *Scheinfeld*, in: MüKo-StGB, § 25 Rn. 39-40.

11 *Haas,* in: Matt/Renzikowski, StGB, § 25 Rn. 5-7; *Scheinfeld*, in: MüKo-StGB, § 25 Rn. 61-64; *Weißer*, in: TK-StGB, § 25 Rn. 3, 4; *Kudlich*, in: BeckOK-StGB, § 25 Rn. 19; *Pohlreich*, in: Lackner/Kühl/Heger, StGB, § 25 Rn. 2-6a.

12 *Kudlich,* in: BeckOK-StGB, § 25 Rn. 44-45.2; *Weißer*, in: TK-StGB, § 25 Rn. 79-82; *Scheinfeld*, in: MüKo-StGB, § 25 Rn. 188; *Kindhäuser/Hilgendorf*, LPK-StGB, 10. Aufl. (2025), § 25 Rn. 47-50.

13 *Weißer*, in: TK-StGB, § 25 Rn. 5; *Schild/Kretschmer*, in: NK-StGB, § 25 Rn. 73; *Scheinfeld*, in: MüKo-StGB, § 25 Rn. 61; *Kudlich*, in: BeckOK-StGB, § 25 Rn. 19; *Pohlreich,* in: Lackner/Kühl/Heger, StGB, § 25 Rn. 2.

14 *Kudlich*, in: BeckOK-StGB, § 25 Rn. 20; *Scheinfeld*, in: MüKo-StGB, § 25 Rn. 62; *Haas,* in: Matt/Renzikowski, StGB, § 25 Rn. 5; *Schild/Kretschmer*, in: NK-StGB, 25 Rn. 73-77.

15 *Kudlich*, in: BeckOK-StGB, § 25 Rn. 20-31.2; *Weißer*, in: TK-StGB, § 25 Rn. 7; *Scheinfeld*, in: MüKo-StGB, § 25 Rn. 65-66; *Pohlreich*, in: Lackner/Kühl/Heger, StGB, § 25 Rn. 4; *Schild/Kretschmer*, in: NK-StGB, § 25 Rn. 86.

16 *Weißer*, in: TK-StGB, Vorb. § 25 Rn. 53-56; *Schild/Kretschmer*, in: NK-StGB, Vorb. § 25 Rn. 5-7; *Pohlreich*, in: Lackner/Kühl/Heger, StGB, Vorb. § 25 Rn. 4-6; *Kindhäuser/Hilgendorf*, LPK-StGB, Vorb. § 25 Rn. 20-39; *Scheinfeld*, in: MüKo-StGB, Vorb. § 25 Rn. 4-5, 10.

17 *Degen/Emmert*, Elektronischer Rechtsverkehr, 3. Aufl. (2025), Rn. 2.

18 *BGH*, Beschl. v. 25.10.2023 – 4 StR 81/23, Rn. 20-21; *Weißer*, in: TK-StGB, § 25 Rn. 8-17; *Schild/Kretschmer*, in: NK-StGB, § 25 Rn. 73-79, 91-94; *Scheinfeld*, in: MüKo-StGB, § 25 Rn. 70-80; *Kudlich*, in: BeckOK-StGB, § 25 Rn. 21-27.1.

19 *Engländer*, in: NK-StGB, § 22 Rn. 36-38; *Bosch*, in: TK-StGB, § 22 Rn. 37-38; *Hoffmann-Holland*, in: MüKo-StGB, § 22 Rn. 112; *Petzsche*/Heger, in: Matt/Renzikowski, StGB, § 22 Rn. 27-31.

Verhalten voraus, das tatbestandsrelevant wird. Technische Systeme bieten hierfür kein Äquivalent. Wo ein System lediglich ausführt, steht nicht eine fremde Person zwischen Täter und Erfolg, sondern nur ein technischer Ablauf.

III. Botnetze und Skripte als „Tatmittler"? – dogmatische Grenzen einer funktionalen Übersetzung

1. Das funktionale Argument

Die Rede von der „Tat durch kompromittierte Systeme" drängt zu einer Parallelisierung. Wie der Hintermann den schuldunfähigen Vordermann lenkt[20], lenkt er das Botnetz; wie der Tatmittler die tatbestandliche Handlung ausführt, versenden die Bots die Pakete oder führen den Schadcode aus.[21] Aus dieser Perspektive soll § 25 Abs. 1 Alt. 2 StGB nicht als personale, sondern als instrumentale Zurechnungsfigur verstanden werden.

Diese Intuition beruht auf einer richtigen Beobachtung (Fernsteuerung), übersetzt sie aber in ein dogmatisch falsches Raster. Denn Fernsteuerung ist kein Spezifikum der mittelbaren Täterschaft. Auch der unmittelbare Täter kann aus der Ferne handeln, etwa, indem er ein System über Netzwerkbefehle manipuliert. Der Unterschied liegt nicht im Abstand, sondern darin, ob ein anderer Mensch als tatbestandsrelevantes Zwischenglied instrumentalisiert wird.[22]

2. Auslegung vs. Analogie

Die Gleichsetzung technischer Mittel mit „anderen" im Sinne des § 25 Abs. 1 Alt. 2 StGB lässt sich nicht ohne Weiteres als teleologische Auslegung legitimieren. Der Normtext differenziert bewusst zwischen „selbst begehen" und „durch einen anderen begehen" und stellt eine Legaldefinition dar.[23] Eine Ausdehnung auf Maschinen würde die Grenze zwischen Auslegung und Analogie überschreiten. Gerade weil § 25 Abs. 1 Alt. 2 StGB keine bloße Beschreibung eines Kausalverlaufs ist, sondern eine Zurechnungsformel, wäre eine solche Analogie mit Blick auf Art. 103 Abs. 2 GG besonders problematisch.[24]

3. Nicht-personale Mittel sind keine Tatmittler

In der Kommentarliteratur wird für Grenzkonstellationen, in denen der vermeintliche Tatmittler kein „intentionales Werkzeug" ist, herausgestellt, dass dann eine unmittelbare Täterschaft naheliegt und eine Behandlung als mittelbare Täterschaft begrifflich überdehnt wäre.[25] Der „Tatmittler" wäre sonst ein bloßer „blinder Kausalfaktor", wie ein mechanisches Werkzeug. Diese Beschreibung trifft die digitale Realität genauer: Der Bot ist nicht Adressat einer Willensherrschaft, sondern ein programmiertes/kompromittiertes Ausführungsmittel.[26]

4. Versuchsbeginn als Lackmustest

Gerade bei automatisierten Prozessen zeigt sich die Gefahr dogmatischer Verschiebungen. Wird der Bot als „Tatmittler" begriffen, liegt es nahe, den Versuchsbeginn an der „Entlassung" dieses Mittlers in die Ausführung zu knüpfen. Für technische Systeme fehlt jedoch ein entsprechendes Konzept. Die Ausführung ist kein menschlicher Entscheidungsakt, sondern ein programmgemäßes Abarbeiten.[27] Der Versuchsbeginn muss daher an der vom Täter gesetzten Gefährdungsnähe orientiert werden[28], wie z.B. Ausführung des Payloads oder Beginn der Paketflut, nicht an einer fiktiven „Mittlerhandlung".

Die Literatur zu Fallenstellungen zeigt, wie sensibel die Anknüpfung ist: diskutiert werden u.a. die Entlassung des Mittlers, der Abschluss der Vorbereitung und die Vornahme einer konkret gefährdenden Handlung. Diese Modelle setzen jedoch eine Person als Mittler voraus und sind nicht ohne Weiteres auf Software übertragbar.[29]

5. Die Gefahr der „Software-Mittäterschaft"

Eine „Digitalisierung" der mittelbaren Täterschaft würdeaußerdem den Weg in eine Metaphorik öffnen, die das Beteiligungssystem überlädt. Wenn Software als Tatmittler gilt, wird die Tatbeherrschung des Hintermannes nicht mehr über personale Defektlagen, sondern über reine Steuerungsfähigkeit definiert. Dann ist jedoch nicht erkennbar, warum § 25 Abs. 1 Alt. 1 StGB nicht ausreichen sollte, da Steuerungsfähigkeit gerade ein Kernargument

---

20 *Schild/Kretschmer*, in: NK-StGB, § 25 Rn. 74, 100; *Weißer*, in: TK-StGB, § 25 Rn. 17; *Kudlich*, in: BeckOK-StGB, § 25 Rn. 27-27.1; *Scheinfeld*, in: MüKo-StGB, § 25 Rn. 64; ZJS, Entscheidungsbesprechung zu *BGH*, Beschl. v. 13.9.2023 – 5 StR 200/23, abrufbar unter: https://bit.ly/4bm94dj (zuletzt abgerufen am 29.1.2026).

21 *Degen/Emmert*, Elektronischer Rechtsverkehr, Rn. 2 (Stichwort: Bot); BSI, Exkurs: Social Bots und Chatbots, abrufbar unter: https://bit.ly/4cogVbv (zuletzt abgerufen am 29.1.2026); SRF, User oder Maschine? KI-Bots fluten das Internet – was das für uns bedeutet, abrufbar unter: https://bit.ly/4l50l2q (zuletzt abgerufen am 29.1.2026); Polizeiliche Kriminalprävention, Botnetze – wenn der Computer zum Zombie wird, abrufbar unter: https://bit.ly/3Nhqyyr (zuletzt abgerufen am 29.1.2026).

22 Merkur, Experten warnen: Diese harmlos wirkende Handlung installiert unbemerkt Schadsoftware auf jedem Gerät, abrufbar unter: https://bit.ly/4b1yBY2 (zuletzt abgerufen am 29.1.2026); Pressetext, aktuelle Warnung: Microsoft-signierte Malware ermöglich gezielte Manipulation des Datenverkehrs, abrufbar unter: https://bit.ly/46IG6ls (zuletzt abgerufen am 29.1.2026).

23 *Weißer*, in: TK-StGB, § 25 Rn. 1; *Schild/Kretschmer*, in: NK-StGB, § 25 Rn. 29; *Scheinfeld*, in: MüKo-StGB, § 25 Rn. 243.

24 *Remmert*, in: Dürig/Herzog/Scholz, GG, 108. EL (08/2025), Art. 103 Abs. 2 Rn. 82–86; *Aust,* in: Huber/Voßkuhle, GG, 8. Aufl. (2024), Art. 103 Rn. 171-172; *Sodan,* in: Sodan, GG, 5. Aufl. (2024), Art. 103 Rn. 20, 21; *Radtke*, in: BeckOK-GG, 64. Ed. (15.6.2025), Art. 103 Rn. 40-41.

25 *Scheinfeld*, in: MüKo-StGB, § 25 Rn. 90-91; *Weißer*, in: TK-StGB, § 25 Rn. 26; *Schild/Kretschmer*, in: NK-StGB, § 25 Rn. 87-90; *Kudlich*, in: BeckOK-StGB, § 25 Rn. 28-30.

26 *Maihold*, in: Ellenberger/Bunte, BankR-HdB, 6. Aufl. (2022), § 33 Rn. 64; *Degen/Emmert*, Elektronischer Rechtsverkehr, Rn. 2.

27 *Degen/Emmert*, Elektronischer Rechtsverkehr, Rn. 2; *Wiebe*, in: Leupold/Wiebe/Glossner, IT-Recht, 4. Aufl. (2021), Rn. 93.

28 *BGH*, Beschl. v. 14.1.2020 – 4 StR 397/19, Rn. 8 ff.; *Bosch*, in: TK-StGB, § 22 Rn. 39-42; *Hoffmann-Holland*, in: MüKo-StGB, § 22 Rn. 112-114.

29 *Schild/Kretschmer*, in: NK-StGB, § 25 Rn. 73-79; *Scheinfeld*, in: MüKo-StGB, § 25 Rn. 179-185; *Ingelfinger*, in: Dölling/Duttge/Rösner, StGB, § 25 Rn. 53-54.

der unmittelbaren Täterschaft im technischen Kontext ist.[30]

Zudem verschiebt sich der Blick von der tatbestandlichen Handlung auf die Projektarchitektur. Wer die Infrastruktur bereitstellt oder die Malware entwickelt, könnte leichter als „mittelbarer Täter“ etikettiert werden, obwohl ihm die konkrete Tatbestandsverwirklichung nicht als eigenes Handeln zugeordnet werden kann. Das ist dogmatisch riskant, weil es die Zurechnung vom Tatbestand löst und in eine allgemeine Verantwortlichkeit für „Cybercrime-Ökosysteme“ umkippen lässt.

6. Zwischenfazit

Botnetze und autonome Skripte sind keine „anderen“ im Sinne des § 25 Abs. 1 Alt. 2 StGB. Sie sind Ausführungsmittel. Die Zurechnung muss daher über unmittelbare Täterschaft und objektive Zurechnung laufen; mittelbare Täterschaft bleibt den personenbezogenen Konstellationen vorbehalten.

IV. Alternativmodelle: unmittelbare Täterschaft, objektive Zurechnung und (begrenzte) Organisationsherrschaft

1. Unmittelbare Täterschaft durch Werkzeuggebrauch: Fernsteuerung als eigene Tathandlung

Wer Malware deployt, Befehle an kompromittierte Systeme sendet oder einen DDoS-Flood startet, „begeht“ die Tat selbst, da er mit dem Versenden der Befehle und dem Start der Aktion die Handlungsherrschaft innehat.[31] Die Handlung liegt in der tatplangemäßen Setzung und Aktivierung des technischen Prozesses. Die Ausführung auf dem Zielsystem ist Teil des beherrschten Kausalverlaufs. Dogmatisch entspricht dies dem Einsatz eines Werkzeugs, das den tatbestandlichen Erfolg herbeiführt.

Diese Einordnung ist nicht nur formal. Sie zwingt dazu, die Täterhandlung konkret zu benennen wie z.B. Übermittlung des Command-Befehls, Ausbringen des Schadcodes oder Konfiguration der Paketflut und den Erfolg als Realisierung eines dadurch geschaffenen Risikos zu prüfen. Der Täter wird nicht „über“ eine technische Zwischeninstanz strafbar, sondern wegen seines eigenen, tatbestandsbezogenen Handelns.

2. Autonomer Code und „Set-and-Forget“

Ein möglicher Einwand lautet, dass der Angreifer nach dem Inverkehrbringen des Schadcodes nicht mehr steuert. Der Code läuft autonom, etwa nach Zeitplan oder ereignisgesteuert. Auch hier ist die Personalisierung des Systems fehl am Platz. Die fehlende Live-Steuerung spricht nicht für mittelbare Täterschaft, sondern ist im Rahmen der objektiven Zurechnung und des Vorsatzes zu bewerten. Maßgeblich ist, ob der Täter die tatbestandliche Gefahr tatplangemäß gesetzt und den Eintritt des Erfolgs zumindest billigend in Kauf genommen hat.

Im digitalen Raum ist daher zwischen zwei Steuerungsdimensionen zu unterscheiden: (i) ex ante Steuerung (Setzen des Prozesses, Parametrisierung) und (ii) ex post Steuerung (Abbruch-/Modulationsmöglichkeiten). Fehlt die ex post Steuerung vollständig, kann dies für die Reichweite des Vorsatzes und die Zurechnung von Exzessen relevant sein; es macht den Täter aber nicht zum mittelbaren Täter.

3. Objektive Zurechnung als Korrektiv

Die objektive Zurechnung ermöglicht es, automatisierte Verläufe normativ zu strukturieren. Sie fragt nach erlaubtem Risiko, Risikoverwirklichung und dem Schutzzweck der Norm. Gerade bei Botnet-Angriffen können Kausalverläufe exzessiv sein, da ein Flood auch Drittsysteme beeinträchtigen kann oder ein Wurm sich schneller ausbreiten kann als geplant. Die Zurechnungsentscheidung darf dann nicht von einer fiktiven „Tatmittlerhandlung“ abhängen, sondern davon, ob sich die vom Täter geschaffene tatbestandsspezifische Gefahr realisiert oder ob ein atypischer Verlauf vorliegt.

4. Eine Zurechnungsmatrix

Für die dogmatische Einordnung digitaler Angriffskonstellationen kann folgende Prüfungslogik als Arbeitsinstrument dienen:

- Liegt ein menschlicher Intermediär vor, der tatbestandsrelevant handelt? → Wenn ja: Prüfung von § 25 Abs. 1 Alt. 2 StGB (Defektlage/Unterordnung) oder Teilnahme.
- Fehlt ein menschlicher Intermediär und wird der tatbestandsrelevante Prozess technisch ausgelöst? → Regel: § 25 Abs. 1 Alt. 1 StGB (Werkzeuggebrauch) mit objektiver Zurechnung.
- Besteht ein arbeitsteiliger menschlicher Organisationsapparat (Austauschbarkeit/regelhaftes Auslösen von Abläufen) und wird die Tat trotz vollverantwortlicher Ausführender „nahezu automatisch“ bewirkt? → Nur dann (und unter Kritikvorbehalt) Diskussion Organisationsherrschaft.
- Sind exzessive, nicht beherrschte Folgeeffekte eingetreten? → Korrektur über objektive Zurechnung und Vorsatzreichweite, nicht über Umdeutung der Täterform.

Diese Matrix ist bewusst restriktiv gegenüber § 25 Abs. 1 Alt. 2 StGB. Sie schützt die Personenbezogenheit der mittelbaren Täterschaft und verschiebt die normative Arbeit dorthin, wo sie hingehört, und zwar in die Zurechnung des tatbestandsrelevanten Risikos und in die Bestimmung des tatbestandlichen Kerngeschehens.

---

30 *Schild/Kretschmer*, in: NK-StGB, § 25 Rn. 23-25, 37; *Scheinfeld*, in: MüKo-StGB, § 25 Rn. 65-66; *Weißer*, in: TK-StGB, § 25 Rn. 22-24; *Haas*, in: Matt/Renzikowski, StGB, § 25 Rn. 33-36; *Ingelfinger*, in: Dölling/Duttge/Rösner, StGB, § 25 Rn. 8.

31 *Weißer*, in: TK-StGB, § 25 Rn. 2; *Scheinfeld*, in: MüKo-StGB, § 25 Rn. 39-41; *Pohlreich,* in: Lackner/Kühl/Heger, StGB, § 25 Rn. 1a; *Kudlich*, in: BeckOK-StGB, § 25 Rn. 18.

5. Organisationsherrschaft: menschliche Apparate vs. technische Regelhaftigkeit

In digitalen Angriffsketten existieren Konstellationen, in denen der Hintermann nicht primär technische Mittel, sondern menschliche Organisationsstrukturen nutzt wie etwa bei arbeitsteiligen „Service"-Modellen (RaaS), in denen Affiliate-Operatoren austauschbar agieren und die Zentrale über Infrastruktur, Schlüsselmaterial oder Auszahlungsmechanismen dispositiv verfügt.

Die Rechtsprechung hat für solche Fälle die Figur der Organisationsherrschaft entwickelt.[32] Trotz vollverantwortlich handelnder Ausführender soll mittelbare Täterschaft möglich sein, wenn der Beitrag des Hintermannes innerhalb bestimmter organisatorischer Rahmenbedingungen regelhafte Abläufe auslöst und nahezu automatisch zur Tatbestandsverwirklichung führt.[33] Diese Konstruktion ist umstritten; kritisiert werden insbesondere Unbestimmtheit und die Gefahr, Beweiserleichterung über Dogmatik zu erzielen.

Auch wenn man Organisationsherrschaft für bestimmte digitale Organisationsmodelle für anschlussfähig hält, muss sie strikt von technischer Automatisierung getrennt werden. Die Regelhaftigkeit eines Programms ist keine Organisationsstruktur im Sinne der Rechtsprechung. Wer technische Regelhaftigkeit mit Organisationsherrschaft gleichsetzt, entkernt den ohnehin umstrittenen Ansatz und macht ihn inhaltsleer.

6. Echte mittelbare Täterschaft über menschliche Intermediäre

Schließlich gibt es digitale Konstellationen, in denen mittelbare Täterschaft klassisch einschlägig ist: Social-Engineering-Angriffe, in denen Menschen als unwissende Ausführende agieren wie z.B. Administratoren, die auf Täuschung hin privilegierte Befehle ausführen, oder Angestellte, die Zugangsdaten preisgeben. Hier ist der Tatmittler als Person vorhanden; sein Defekt (Irrtum, fehlender Vorsatz) kann die Tatbeherrschung des Hintermannes begründen.[34] Die digitale Besonderheit liegt dann nicht in der Abwesenheit des Tatmittlers, sondern im Kommunikationsmedium.

V. Tatbestandliche Implikationen und Fallkonstellationen (insb. §§ 303a, 303b StGB)

1. Datenveränderung (§ 303a StGB)

§ 303a StGB schützt Daten als nicht unmittelbar wahrnehmbare Informationen, an denen ein fremdes Nutzungsrecht besteht; geschützt sind auch Programme und Programmteile.[35] Die Tathandlungen wie Löschen, Unterdrücken, Unbrauchbarmachen oder Verändern bilden den tatbestandlichen Kern und können auch durch Unterlassen verwirklicht werden, wenn ein Garant die drohende Datenveränderung nicht abwendet.[36]

Botnet- oder Malware-Angriffe realisieren § 303a StGB typischerweise durch automatisierte Manipulationen, indem Dateien verschlüsselt (Unbrauchbarmachen)[37], Logfiles überschrieben (Verändern/Löschen)[38] oder Zugriffe blockiert (Unterdrücken)[39] werden. Dogmatisch ist dabei die Zurechnung nicht deshalb problematisch, weil die Ausführung technisch vermittelt ist, sondern weil sie automatisiert erfolgt. Die Lösung liegt darin, die Programmausführung als vom Täter gesetzten Prozess zu behandeln. Die „Tat" wird nicht von einem anderen Menschen ausgeführt, sondern vom Täter selbst, indem er den Code zur Ausführung bringt.

Dass dies keine bloße Theorie ist, zeigt bereits die Beschreibung der Tathandlungen. Das vorsätzliche Installieren eines Killer- oder Virusprogramms wird als Beispiel für tatbestandliches Löschen genannt; Unbrauchbarmachen kann durch Programmsperren, Einfügungen oder Überschreiben erfolgen.[40]

2. Vorbereitung und Vorfeld: gesetzgeberische Signale

Bemerkenswert ist, dass der Gesetzgeber für digitale Delikte teilweise eigene Vorfelddelikte bzw. Vorbereitungstatbestände geschaffen hat. § 303a Abs. 3 StGB wurde eingefügt, um besonders gefährliche Vorbereitungshandlungen im Hinblick auf Eingriffe in Daten unter Strafe zu

---

32 *BGH*, Beschl. v. 2.11.2007 – 2 StR 384/07, Rn. 6.; *Schild/Kretschmer*, in: NK-StGB, § 25 Rn. 38-44; *Weißer*, in: TK-StGB, § 25 Rn. 29-30; *Kudlich*, in: BeckOK-StGB, § 25 Rn. 28-30, 34-35.1; *Scheinfeld*, in: MüKo-StGB, § 25 Rn. 199-207.

33 *Weißer*, in: TK-StGB, § 25 Rn. 36-40; *Scheinfeld*, in: MüKo-StGB, § 25 Rn. 147-154; *Schild/Kretschmer*, in: NK-StGB, § 25 Rn. 106-109.

34 *Haas,* in: Matt/Renzikowski, StGB, § 25 Rn. 49-52; *Scheinfeld*, in: MüKo-StGB, § 25 Rn. 65-66; *Kindhäuser/Hilgendorf*, in: LPK-StGB, § 25 Rn. 7-10; *Schild/Kretschmer*, in: NK-StGB, § 25 Rn. 87-90; *Kudlich*, in: BeckOK-StGB, § 25 Rn. 13-16.

35 *Hecker*, in: TK-StGB, § 303a Rn. 1; *Wieck-Noodt*, in: MüKo-StGB, § 303a Rn. 1-4; *Basar/Heinelt*, in: ComputerR-HdB, 40. EL (März 2025), Teil 10. 100. Rn. 125; *Weidemann*, in: BeckOK-StGB, § 303a Rn. 2-2.2; *Heger*, in: Lackner/Kühl/Heger, StGB, § 303a Rn. 1; *Schallbruch*, in: Hornung/Schallbruch, IT-Sicherheitsrecht, 2. Aufl. (2024), Rn. 15–23.

36 *Weidemann*, in: BeckOK-StGB, § 303a Rn. 8-15.1; *Wieck-Noodt*, in: MüKo-StGB, § 303a Rn. 11; *Hecker*, in: TK-StGB, § 303a Rn. 4-8; *Bär*, in: WirtschaftsStrafR-HdB, 6. Aufl. (2025), 15. Kap. Rn. 114-118; *Wengenroth*, in: DatenschutzsanktionenR-HdB, 2023, § 20 Rn. 15-17.

37 *Hecker*, in: TK-StGB, § 303a Rn. 7; *Weidemann*, in: BeckOK-StGB, § 303a Rn. 13-14; *Wieck-Noodt*, in: MüKo-StGB, § 303a Rn. 14; *Heger,* in: Lackner/Kühl/Heger, StGB, § 303a Rn. 3; *Kargl*, in: NK-StGB, § 303a Rn. 11.

38 *Weidemann*, in: BeckOK-StGB, § 303a Rn. 9-10, 15-15.1; *Basar/Heinelt*, in: ComputerR-HdB, Teil 10. 100. Rn. 134; *Wieck-Noodt*, in: MüKo-StGB, § 303a Rn. 12, 15; *Hecker*, in: TK-StGB, § 303a Rn. 5, 8.

39 *Hecker*, in: TK-StGB, § 303a Rn. 6; *Bär*, in: WirtschaftsStrafR-HdB, 15. Kap. Rn. 116; *Weidemann*, in: BeckOK-StGB, § 303a Rn. 11-12.2; *Wengenroth*, in: Klaas/Momsen/Wybitul, DatenschutzsanktionenR-HdB, § 20 Rn. 19-20.

40 *Bär*, in: WirtschaftsStrafR-HdB, 15. Kap. Rn. 115; *Wieck-Noodt*, in: MüKo-StGB, § 303a Rn. 12; *Reinbacher*, in: NK-WSS, 2. Aufl. (2022), § 303a Rn. 27; *Kargl*, in: NK-StGB, § 303a Rn. 9; *Weidemann*, in: BeckOK-StGB, § 303a Rn. 10.

stellen.[41] Gerade diese gesetzgeberische Entscheidung spricht gegen ein Bedürfnis, Vorfeldprobleme über eine Ausdehnung von § 25 Abs. 1 Alt. 2 StGB zu lösen. Wo der Gesetzgeber Vorverlagerung will, normiert er sie – und begrenzt sie zugleich.

3. Computersabotage (§ 303b StGB)

§ 303b StGB schützt als Sondertatbestand das Interesse der Betreiber und Nutzer an der ordnungsgemäßen Funktionsweise von Datenverarbeitungen;[42] das Delikt ist ein Erfolgsdelikt, weshalb eine bloße Gefährdung nicht genügt.[43] Tatobjekt ist eine Datenverarbeitung, deren Begriff weit zu verstehen ist und auch den weiteren Umgang mit Daten und deren Verwertung umfasst; das Merkmal der „wesentlichen Bedeutung“ dient als Filter gegen Bagatellen.[44] Der Erfolg liegt in der erheblichen Störung, die den reibungslosen Ablauf nicht unerheblich beeinträchtigt; eine bloße Gefährdung reicht nicht.[45]

DDoS-Angriffe über Botnetze illustrieren, dass die Erfolgsherbeiführung häufig ein Systemeffekt ist. Es genügt bereits, wenn ein konkreter Datenverarbeitungsvorgang infolge der Tat nicht in bisheriger Form durchgeführt werden kann, sofern die Wiederherstellung nicht ohne großen Aufwand gelingt. Der Angreifer setzt die Paketflut in Gang, wählt das Ziel und moduliert die Last.[46] Das spricht nicht für mittelbare Täterschaft, sondern für unmittelbare Täterschaft (Werkzeuggebrauch) mit erfolgsbezogener objektiver Zurechnung.

Für Versuch und Vollendung ist § 303b StGB besonders instruktiv. Nicht jedes unmittelbare Ansetzen zur Sabotagehandlung stellt schon den Versuch der Computersabotage dar, weil der tatbestandliche Erfolg, also die Störung eines konkreten Datenverarbeitungsvorgangs, erforderlich bleibt. Die Versuchsschwelle ist daher stärker erfolgsnah.

Hinzu tritt, dass § 303b Abs. 5 StGB in Verbindung mit § 202c StGB Vorbereitungshandlungen selbständig unter Strafe stellt und sogar ein tätige-Reue-ähnliches Korrektiv vorsieht.[47] Auch dies ist ein Signal, da die Vorverlagerung normiert wird, aber in einem eigenen, systematisch abgegrenzten Instrument. Eine dogmatische Umgehung über § 25 Abs. 1 Alt. 2 StGB würde diese Systementscheidung unterlaufen.

4. Ransomware als Herrschaftsindikator ohne Tatmittlerfiktion

Ransomware-Angriffe zeigen, dass die dogmatisch zentrale Herrschaft nicht im „Ausführen“ (Verschlüsseln) liegt, sondern in der Kontrolle des Fortbestands der Beeinträchtigung. Der Angreifer kann, durch Schlüsselmaterial oder Kill-Switch, über Aufrechterhaltung und Beendigung disponieren.[48] Diese Steuerungsposition ist dogmatisch anschlussfähig, ohne dass das Zielsystem als Tatmittler personalisiert werden müsste.

Technisch ist dies durch hybride Verschlüsselungsarchitekturen begünstigt: Dateien werden lokal symmetrisch verschlüsselt; der Schlüssel wird asymmetrisch gesichert, wobei der private Schlüssel typischerweise auf Angreifer-Infrastruktur verbleibt.[49]

5. Fallbeispiele (schematisch)

Zur Illustration lassen sich drei Konstellationen unterscheiden:

a) Botnet-DDoS

Der Täter mietet Botnet-Kapazität, setzt Ziel und Dauer und startet den Flood. Tatbegehung ist unmittelbar (§ 25 Abs. 1 Alt. 1 StGB); die Bots sind Werkzeuge. Versuch/Vollendung richten sich nach §303b-Erfolg.

b) Ransomware-Affiliate

Ein Developer stellt Code, ein Affiliate deployt, die Zentrale verwaltet Schlüssel und Zahlungsabwicklung. Hier können neben unmittelbarer Täterschaft der Deployenden

---

41 *Bär*, in: WirtschaftsStrafR-HdB, 15. Kap. Rn. 122, 123; *Wieck-Noodt*, in: MüKo-StGB, § 303a Rn. 7; *Hecker*, in: TK-StGB, § 303a Rn. 12; *Weidemann*, in: BeckOK-StGB, § 303a Rn. 16; *Kargl*, in: NK-StGB, § 303a Rn. 18.

42 *BGH*, Beschl. v. 11.1.2017 – 5 StR 164/16, Rn. 19; *Weidemann*, in: BeckOK-StGB, § 303b Rn. 4, 4.1; *Bär*, in: WirtschaftsStrafR-HdB, 15. Kap. Rn. 128-130a; *Wieck-Noodt*, in: MüKo-StGB, § 303b Rn. 7-9; *Hecker*, in: TK-StGB, § 303b Rn. 2, 3; *Kargl*, in: NK-StGB, § 303b Rn. 4; *Gercke,* in: Spindler/Schuster/Kaesling, StGB, 5. Aufl. (2026), § 303b Rn. 2-4.

43 *Hecker*, in: TK-StGB, § 303b Rn. 1; *Wieck-Noodt*, in: MüKo-StGB, § 303b Rn. 2; *Bär*, in: WirtschaftsStrafR-HdB, 15. Kap. Rn. 125; *Brodowski*, in: Kipker Cybersecurity-HdB, 2. Aufl. (2023), Kap. 17 Rn. 36; *Basar/Heine,* in: ComputerR-HdB, Teil 10. 100. Rn. 142.

44 *Basar/Heinelt*, in: ComputerR-HdB, Teil 10. 100. Rn. 146-148; *Weidemann*, in: BeckOK-StGB, § 303b Rn. 5-9; *Wieck-Noodt*, in: MüKo-StGB, § 303b Rn. 23; *Gercke*, in: Spindler/Schuster/Kaesling, StGB, § 303b Rn. 5; *Bär*, in: WirtschaftsStrafR-HdB, 15. Kap. Rn. 126, 127; *Altenhain,* in: Matt/Renzikowski, StGB, § 303b Rn. 14.

45 *Weidemann*, in: BeckOK-StGB, § 303b Rn. 15, 16; *Wieck-Noodt*, in: MüKo-StGB, § 303b Rn. 19; *Bär*, in: WirtschaftsStrafR-HdB, 15. Kap. Rn. 32; *Altenhain,* in: Matt/Renzikowski, StGB, § 303b Rn. 4, 5; *Hecker*, in: TK-StGB, § 303b Rn. 9.

46 *Bär*, in: WirtschaftsStrafR-HdB, 15. Kap. Rn. 130-130a; *Weidemann*, in: BeckOK-StGB, § 303b Rn. 15; *Hecker*, in: TK-StGB, § 303b Rn. 9; *Altenhain*, in: Matt/Renzikowski, StGB, § 303b Rn. 7, 8; *Heger,* in: Lackner/Kühl/Heger, StGB, § 303b Rn. 5.

47 *Bär*, in: WirtschaftsStrafR-HdB, 15. Kap. Rn. 140; *Grözinger*, in: MAH Strafverteidigung, 3. Aufl. (2022), § 50 Rn. 77; *Heger,* in: Lackner/Kühl/Heger, StGB, § 303b Rn. 9; *Weidemann*, in: BeckOK-StGB, § 303b Rn. 20; *Hecker*, in: TK-StGB, § 303b Rn. 21; *Altenhain,* in: Matt/Renzikowski, StGB, § 303b Rn. 13; *Gercke,* in: Spindler/Schuster/Kaesling, StGB, § 303b Rn. 12.

48 *BGH*, Beschl. v. 8.4.2021 – 1 StR 78/21, Rn. 19; BSI, Ransomware – Fakten und Abwehrstrategien, abrufbar unter: https://bit.ly/4bjBO6B (zuletzt abgerufen am 29.1.2026), *Bär*, in: WirtschaftsStrafR-HdB, 15. Kap. Rn. 116, 140.

49 *Beaman/Barkworth*, Computers & Security 111 (2021) 102490, insb. S. 2–3; BORN CITY vom 25.1.2026, Osiris-Ransomware nutzt gefährliche BYOVD-Methode, abrufbar unter: https://bit.ly/3N2OwgP (zuletzt abgerufen am 29.1.2026); BSI vom 16.2.2025, Cyberaggression: Hybride Bedrohungen des 21. Jahrhunderts und wie wir uns vor ihnen schützen, abrufbar unter: https://bit.ly/4d1zsul (zuletzt abgerufen am 29.1.2026).

mittäterschaftliche oder organisationsbezogene Zurechnungsfragen auftreten; mittelbare Täterschaft „durch Systeme“ ist jedoch nicht notwendig.

c) Social Engineering

Ein Mitarbeiter wird getäuscht und führt ein Skript aus, das Daten löscht. Hier kann mittelbare Täterschaft über einen menschlichen Tatmittler einschlägig sein.

6. Kurzer Ausblick auf § 263a StGB (Computerbetrug)

Auch bei § 263a StGB werden Eingaben und Datenverarbeitungen oft skriptgesteuert manipuliert wie z.B. automatisierte Transaktionen oder Credential-Stuffing.[50] Die Zurechnung ist auch hier primär eine Frage der unmittelbaren Täterschaft und objektiven Zurechnung. Der Täter bewirkt durch Eingaben oder Programmsteuerung die unrichtige bzw. unvollständige Datenverarbeitung. Mittelbare Täterschaft ist nur dort erforderlich, wo menschliche Zwischenakte wie etwa unwissende Kontoinhaber oder Mitarbeiter tatbestandsrelevante Handlungen ausführen.

7. Ausblick: Autonome Angriffsroutinen

(1) Die Diskussion gewinnt zusätzliche Schärfe, wenn Angriffsroutinen nicht nur automatisiert, sondern adaptiv sind wie z.B. dynamische Zielauswahl oder selbständige Privilegieneskalation. Gerade dann ist Zurückhaltung gegenüber einer Personalisierung technischer Systeme angezeigt. Die Zurechnung muss über Vorsatz, objektive Zurechnung und ggf. Fahrlässigkeitsdelikte gesteuert werden. Eine Erweiterung des § 25 Abs. 1 Alt. 2 StGB würde hingegen die dogmatischen Probleme nur verschieben, nicht lösen.

(2) Täterhandlung ist die tatplangemäße Setzung bzw. Steuerung des technischen Prozesses; die tatbestandliche Erfolgszurechnung erfolgt über objektive Zurechnung (Risikoverwirklichung, Schutzzweck).

(3) Mittelbare Täterschaft kommt nur dort in Betracht, wo Menschen defizitär oder strukturell untergeordnet handeln (insbesondere Social Engineering).

(4) Organisationsherrschaft kann, sofern anerkannt, nur gegenüber menschlichen Organisationsapparaten und unter strengen Voraussetzungen diskutiert werden; technische Regelhaftigkeit genügt nicht.

8. Organisationsstrukturen in Cybercrime-Modellen: Abgrenzungslinien zur Organisationsherrschaft

Ein eigener Grenzbereich entsteht bei arbeitsteiligen Geschäftsmodellen (etwa Ransomware-as-a-Service), in denen menschliche Operatoren austauschbar agieren, während zentrale Akteure Infrastruktur, Schlüsselmaterial und Auszahlungsmechanismen kontrollieren. In solchen Konstellationen kann die Diskussion um organisationsbezogene Zurechnungsmodelle zwar naheliegen. Gleichwohl ist strikt zu trennen: Die Frage, ob eine Tat „durch einen anderen“ begangen wird, ist eine Frage personenbezogener Vermittlung; die Frage, ob eine Organisation tatbestandsrelevante Abläufe regelhaft auslöst, betrifft ein spezifisches Herrschaftsmodell gegenüber Menschen, nicht gegenüber Maschinen.[51] Für die dogmatische Einordnung empfiehlt es sich, zunächst die tatbestandliche Kernhandlung zu identifizieren, also bei § 303a StGB die Datenbeeinträchtigung und bei § 303b StGB die erhebliche Störung, und sodann zu prüfen, wer im konkreten Tatprogramm darüber disponiert: Wer bestimmt Ziel, Zeitpunkt, Intensität, Abbruch? Wer hält technische Schlüsselpositionen wie Schlüsselverwaltung, C2-Kontrolle oder Kill-Switch? Diese Kriterien können innerhalb einer Mittäter- oder (eng begrenzten) organisationsbezogenen Zurechnung relevant sein. Sie sprechen aber gerade nicht dafür, die kompromittierten Systeme als Tatmittler zu behandeln. Das System bleibt Werkzeug; die Zurechnung spielt sich auf der Ebene menschlicher Rollen und Verantwortungsbeziehungen ab. Gerade im digitalen Raum ist zudem zu beachten, dass arbeitsteilige Strukturen häufig modular und marktartig organisiert sind. Wo lediglich standardisierte Leistungen „eingekauft“ werden (Botnet-Miete, Exploit-Pakete, Hosting), fehlt es häufig an der reziproken Bindung, die täterschaftliche Zurechnung im engeren Sinne rechtfertigt. Nach ständiger Rechtsprechung des *BGH* ist die Frage der Handlungseinheit oder -mehrheit nach dem individuellen Tatbeitrag eines jeden Beteiligten zu beurteilen.[52] Auch insoweit ist der Versuchung zu widerstehen, über § 25 Abs. 1 Alt. 2 StGB eine projektbezogene Gesamtverantwortung zu konstruieren.

Zurechnungsdruck, Attribution und die Versuchung dogmatischer Abkürzungen Digitale Angriffe sind häufig gerade deshalb erfolgreich, weil sie Zurechnung und Nachweis erschweren. Der Angreifer bedient sich kompromittierter Geräte als Verkehrsträger, verschleiert Kommunikationswege und trennt Infrastruktur, Ausführung und Monetarisierung organisatorisch. Für die Strafrechtsdogmatik besteht hier ein doppelter Druck. Einerseits besteht das legitime Bedürfnis, den „Hintermann“ als Täter zu erfassen, auch wenn die Ausführung nicht sichtbar „von Hand“ erfolgt. Andererseits darf die Dogmatik nicht zum Ersatz für technische Attribution werden. Die Einordnung kompromittierter Systeme als „Tatmittler“ hätte (scheinbar) den Vorteil einer einfachen Beschreibung. Die „Tathandlung“ geschieht durch die Bots, der Hintermann sei deshalb mittelbarer Täter. Damit würde jedoch das Kernproblem nur sprachlich umetikettiert.

Dogmatisch ist die Zurechnung nicht deshalb schwierig, weil der Tatmittler fehlt, sondern weil täterseitige Steuerungshandlungen, wie etwa das Ausbringen der Malware, die Parametrisierung des Floods, die Verwaltung von

---

[50] *Noll*, in: MüKo-StGB, § 263a Rn. 1, 2; *Schmidt*, in: BeckOK-StGB, § 263a Rn. 2, 6-9, 37-40; *Bär*, in: WirtschaftsStrafR-HdB, 15. Kap. Rn. 11; *Heger,* in: Lackner/Kühl/Heger, StGB, § 263a Rn. 5-15; *Noll*, in: MüKo-StGB, § 263a Rn. 41-42; *Kindhäuser/Hoven*, in: NK-StGB, § 263a Rn. 10-12.

[51] *Schild/Kretschmer*, in: NK-StGB, § 25 Rn. 38; *Weißer*, in: TK-StGB, § 25 Rn. 29-30, 43-45; *Scheinfeld*, in: MüKo-StGB, § 25 Rn. 147-149; *Kudlich*, in: BeckOK-StGB, § 25 Rn. 28-30.

[52] *BGH*, Beschl. v. 8.4.2021 – 1 StR 78/21, Rn. 20 ff.

Schlüsseln oder das Betreiben der Command-and-Control-Infrastruktur, in den Ermittlungen häufig nur indirekt rekonstruierbar sind. Die richtige Antwort liegt daher in einer Normierung der Zurechnungskriterien (Werkzeuggebrauch und objektive Zurechnung) und in einer forensischen Rekonstruktion dieser Steuerungsakte, nicht in einer „Software-Mittäterschaft“.

Dies gilt umso mehr, als expansive Täterkonstruktionen die Differenzierung zwischen Täterschaft und Teilnahme unterlaufen können. Wer lediglich Zugang zu einem Botnetz bereitstellt, wird nicht dadurch Täter der späteren Computersabotage, dass Bots Pakete versenden. Ob ein solcher Akteur Täter, Mittäter oder Teilnehmer ist, hängt vielmehr von Tatplanbindung, Beitragsherrschaft und Vorsatz ab. Die dogmatische Trennung schützt deshalb nicht nur das Bestimmtheitsgebot, sondern auch die schuldangemessene Individualisierung strafrechtlicher Verantwortung.

9. Versuchsbeginn und Rücktritt im automatisierten Geschehen

Die bislang skizzierte Versuchsdogmatik lässt sich durch zwei Beobachtungen präzisieren. Erstens verschiebt Automatisierung das Gewicht von „Handlungsnähe“ zu „Gefährdungsnähe“. Bei DDoS-Angriffen ist das unmittelbare Ansetzen nicht die vorherige Inbetriebnahme des Botnetzes, sondern der tatplangemäße Start eines Floods gegen ein konkret adressiertes Zielsystem. Das Auslösen der Paketflut ist funktional dem Betätigen eines Auslösers vergleichbar; der nachfolgende Datenverkehr ist – strafrechtlich – der beherrschte Kausalverlauf. Ähnliches gilt bei Ransomware: Das bloße Bereithalten von Schadsoftware ist noch Vorbereitung; das unmittelbare Ansetzen beginnt mit der Ausführung der Verschlüsselungsroutine oder mit dem Schritt, der nach dem Tatplan ohne weitere Zwischenschritte zur Datenunbrauchbarkeit führt.

Zweitens wird die Rücktrittsdogmatik im Digitalen häufig an Abbruch- und Steuerungspositionen konkretisiert. Wer über ein Botnetz verfügt, kann – jedenfalls typischerweise – Stop-Kommandos erteilen oder C2-Knoten abschalten; wer im Ransomware-Kontext Schlüsselmaterial kontrolliert, kann die tatbestandliche Beeinträchtigung beenden oder zumindest abmildern. Diese Möglichkeiten sind rechtlich relevant, weil sie zeigen, dass das Tatgeschehen auch nach Beginn der Ausführung noch steuerbar ist. Im Rücktritt ist dann zu fragen, ob der Täter den Erfolg verhindert oder sich ernsthaft darum bemüht; bei fortdauernden Beeinträchtigungen wie z.B. anhaltender DDoS kann das Abbruchverhalten auch für die Dauer- und Schadensdimension der Tat von Bedeutung sein.

Die zentrale Pointe für die hier diskutierte Täterform ist: Weder Versuchsbeginn noch Rücktritt benötigen einen „Tatmittler“ als Adressaten. Sie lassen sich – systemkonform – als Steuerungsfragen gegenüber dem vom Täter selbst gesetzten technischen Prozess behandeln. Damit wird zugleich die unproduktive Alternative vermieden, entweder § 25 Abs. 1 Alt. 2 StGB auf Systeme auszudehnen oder aber digitale Angriffsszenarien dogmatisch als „handlungsfern“ zu behandeln. Das Werkzeugmodell erlaubt eine präzise, tatbestandliche Anknüpfung.

10. Systematische Einordnung: Vorverlagerung und Deliktsspezifika statt Täterausweitung

Die Diskussion um mittelbare Täterschaft durch Systeme ist häufig auch Ausdruck eines kriminalpolitischen Bedürfnisses. Digitale Angriffe entstehen aus Vorbereitungshandlungen[53] wie Scans, Exploit-Entwicklung oder Botnet-Aufbau, deren Gefährlichkeit offensichtlich ist, während eine Teilnahme an der späteren Haupttat nicht immer nachweisbar oder – wegen fehlender Tatplanbindung – dogmatisch begründbar ist. Diese Lücke darf jedoch nicht durch eine Ausweitung des Täterbegriffs geschlossen werden. Zum einen würden dadurch die Zurechnungsgrenzen zwischen Täter- und Teilnehmerverantwortlichkeit verwischt. Zum anderen hat der Gesetzgeber gerade im digitalen Bereich gezeigt, dass er die Vorfeldstrafbarkeit punktuell und begrenzt normiert.

Das spricht dafür, systematische Probleme auf der Ebene von Deliktsspezifika wie Vorbereitungstatbestände, Erfolgsstruktur und Versuchsschwelle zu lösen, nicht durch eine Umdeutung des § 25 StGB. Für die Praxis bedeutet dies, dass in Botnet-Konstellationen zunächst sauber zu bestimmen ist, welches Delikt tatbestandlich im Raum steht (z.B. § 303b StGB bei DDoS-Störung, § 303a StGB bei Datenmanipulation). Sodann ist zu klären, welche Steuerungshandlungen dem Beschuldigten zurechenbar sind (Befehle, Parametrisierung, Schlüsselverwaltung). Erst im dritten Schritt sind Zurechnungsformen zu prüfen wie unmittelbare Täterschaft, Mittäterschaft, Teilnahme und ggf. vorbereitende Delikte. Eine Abkürzung über „mittelbare Täterschaft durch Systeme“ ist demgegenüber dogmatisch unpräzise und birgt, gerade bei neutralen oder marktartigen Beiträgen, erhebliche Überdehnungsrisiken.

11. Ausblick: Autonomiegrade und „KI-gestützte“ Angriffsroutinen

Die hier vertretene Begrenzung der mittelbaren Täterschaft wird in Zukunft eher an Bedeutung gewinnen. Mit zunehmender Automatisierung und adaptiven Angriffsroutinen wie z.B. dynamische Ausbreitung, automatisiertes Privilegien-Management oder selbständige Wahl von Angriffspfaden steigt die Versuchung, technische Prozesse als „quasi-personale“ Mittler zu behandeln. Strafrechtsdogmatisch ist hiervor zu warnen, denn je mehr ein System adaptiv reagiert, desto weniger trägt eine Anthropomorphisierung zur Klarheit bei. Die entscheidenden Zurechnungsfragen werden vielmehr verschoben – nämlich auf Vorsatz und objektive Zurechnung.

[53] *Hecker*, in: TK-StGB, § 303a Rn. 12; *Heger,* in: Lackner/Kühl/Heger, § 303a Rn. 1-7; *Graf*, in: MüKo-StGB, § 202c Rn. 1-3a; *Eisele*, in: TK-StGB, § 202c Rn. 5.

So ist bei hochautonomen Routinen besonders sorgfältig zu prüfen, ob sich noch die vom Täter geschaffene tatbestandsspezifische Gefahr realisiert oder ob ein atypischer Verlauf vorliegt, der außerhalb des tatplangemäß beherrschten Risikos liegt. Gleiches gilt für die Reichweite des Vorsatzes. Die Tatsache, dass ein Programm unter bestimmten Bedingungen „selbständig" eskaliert, kann die Annahme eines Vorsatzexzesses oder, je nach Delikt, die Relevanz fahrlässiger Begehungsformen nahelegen. Das ist dogmatisch anspruchsvoll, aber systematisch sauber. Eine Ausdehnung des § 25 Abs. 1 Alt. 2 StGB würde diese Fragen nicht lösen, sondern verdecken. Die Unschärfe würde in die Täterform verlagert, statt die normativen Kriterien dort anzuwenden, wo sie hingehören. Gerade im digitalen Raum ist jedoch Transparenz der Zurechnung zentral – nicht zuletzt, weil sich strafrechtliche Verantwortung häufig an der Schnittstelle zwischen deliktischer Nutzung und neutraler Technik entfaltet. Das Strafrecht sollte deshalb an der Personenbezogenheit der mittelbaren Täterschaft festhalten und technische Autonomie als Problem von Risiko, Vorsatz und Tatbestandsbezug behandeln.

12. Kriminalpoltische Implikationen

Die vorstehende Analyse lässt drei kriminalpolitische Schlussfolgerungen zu. Erstens wäre eine – auch nur stillschweigende – Ausdehnung des § 25 Abs. 1 Alt. 2 StGB auf technische Durchführungsmittel kriminalpolitisch kontraproduktiv. Sie würde die Bestimmtheit des Beteiligungssystems untergraben und den Weg zu einer diffusen „Projektverantwortlichkeit" für Cybercrime-Infrastrukturen ebnen, die mit dem Schuldprinzip schwer vereinbar ist. Der rechtsstaatliche Preis einer solchen Abkürzung stünde in keinem Verhältnis zum kriminalpolitischen Ertrag, zumal die bestehenden dogmatischen Instrumente - unmittelbare Täterschaft durch Werkzeuggebrauch, Mittäterschaft bei arbeitsteiligen Modellen, Teilnahme und punktuelle Vorbereitungstatbestände – eine lückenlose und differenzierte Erfassung digitaler Angriffsszenarien ermöglichen.

Zweitens bestätigt die Untersuchung, dass der Gesetzgeber im Bereich der Cyberkriminalität eine bewusste Systementscheidung getroffen hat: Wo Vorverlagerung kriminalpolitisch geboten erscheint, normiert er sie in eigenständigen, tatbestandlich begrenzten Instrumenten (§§ 202c, 303a Abs. 3, 303b Abs. 5 StGB). Dieses legislatorische Signal spricht dagegen, Vorfeldprobleme über eine Überdehnung der Täterfigur zu lösen.

Drittens verdient die forensisch-ermittlungspraktische Dimension Beachtung. Die Attraktivität expansiver Täterkonstruktionen erklärt sich häufig daraus, dass die technische Attribution - also die Zuordnung konkreter Steuerungshandlungen zu identifizierbaren Personen - bei digitalen Angriffen besonders schwierig ist. Die Dogmatik darf jedoch nicht zum Ersatz für forensische Aufklärung werden. Kriminalpolitisch wäre es daher vorzugswürdig, in den Ausbau technischer Ermittlungskapazitäten und in die Konkretisierung der Zurechnungskriterien (Werkzeuggebrauch, objektive Zurechnung) zu investieren, statt die Zurechnungsgrenzen des Beteiligungssystems aufzuweichen. Auch die europäische Dimension ist in den Blick zu nehmen: Da Botnet-Infrastrukturen regelmässig grenzüberschreitend operieren, stellt sich die Frage, ob eine Harmonisierung der beteiligungsrechtlichen Zurechnungsmassstäbe im europäischen Strafrecht – etwa im Rahmen der Cybercrime-Konvention oder künftiger EU-Richtlinien - kriminalpolitisch geboten ist.

13. Schlussbemerkung: Dogmatische Ökonomie und Begriffsdisziplin

Die vorgeschlagene Begrenzung ist nicht „dogmatischer Formalismus", sondern Ausdruck dogmatischer Ökonomie. § 25 Abs. 1 Alt. 2 StGB erfüllt eine spezifische Funktion: die Täterzurechnung über eine Person als defizitäres oder untergeordnetes Ausführungs-Zwischenglied. Wird diese Funktion auf technische Prozesse ausgedehnt, verschiebt sich die Zurechnungsarbeit in eine begriffliche Zone, in der die klassischen Konturen wie Defekt, Herrschaft über eine Person oder Verantwortungsgefälle fehlen. Die Folge ist nicht mehr „Modernität", sondern Unschärfe. Umgekehrt zeigt der digitale Kontext, dass das Strafrecht über hinreichende Instrumente verfügt: unmittelbare Täterschaft über Werkzeuggebrauch, objektive Zurechnung, Mittäterschaft/Teilnahme für arbeitsteilige Rollenbeiträge sowie punktuelle Vorbereitungstatbestände. Die Aufgabe der Dogmatik besteht darin, diese Instrumente konsequent am tatbestandlichen Kerngeschehen auszurichten und Zurechnung transparent zu begründen. Genau darin liegt der rechtsstaatliche Mehrwert einer begriffsdisziplinierten Lösung.

VI. Ergebnis: Kriterien und Grenzen

Die Untersuchung hat gezeigt, dass § 25 Abs. 1 Alt. 2 StGB eine personenbezogene Zurechnungsfigur ist und bleibt. Der Wortlaut „durch einen anderen" meint einen menschlichen Tatmittler, dessen Defektlage oder strukturelle Unterordnung die Tatherrschaft des Hintermannes begründet. Kompromittierte Systeme – Botnetze, Skripte, autonome Routinen – erfüllen diese Voraussetzung nicht. Ihnen fehlt die Eigenschaft, Adressat einer Willensherrschaft zu sein; sie irren nicht, handeln nicht vorsätzlich und tragen kein normatives Defizit. Die Gleichsetzung technischer Ausführungsmittel mit Tatmittlern würde daher die Grenze zwischen Auslegung und Analogie überschreiten und die Begrenzungsfunktion des Beteiligungssystems preisgeben.

Digitale Angriffe über automatisierte Prozesse sind vielmehr als unmittelbare Täterschaft gemäß § 25 Abs. 1 Alt. 1 StGB einzuordnen. Der Täter begeht die Tat selbst, indem er den tatbestandsrelevanten technischen Prozess in Gang setzt und steuert – sei es durch das Ausbringen von Schadcode, das Konfigurieren einer Paketflut oder das Aktivieren einer Verschlüsselungsroutine. Dass die Ausführung sodann automatisiert erfolgt, ändert an der Täterqualität nichts; es verlagert die normative Arbeit lediglich in die objektive Zurechnung, die abweichende oder exzessive Verläufe als Frage der Risikoverwirklichung und des

Schutzzwecks der Norm behandelt. Echte mittelbare Täterschaft bleibt hingegen den Konstellationen vorbehalten, in denen ein menschlicher Intermediär tatbestandsrelevant handelt – etwa beim Social Engineering, bei irrtumsbedingter Ausführung oder unter Zwangslagen. Nur dort ist das Zurechnungsmodell des § 25 Abs. 1 Alt. 2 StGB funktional einschlägig.

Auch die Figur der Organisationsherrschaft bietet keinen Anknüpfungspunkt für eine Personalisierung technischer Systeme. Soweit man ihr folgt, setzt sie einen menschlichen Organisationsapparat voraus, in dem der Hintermann organisationsbezogene Rahmenbedingungen ausnutzt und die Tatbestandsverwirklichung durch austauschbare Ausführende regelhaft auslöst. Ein Botnetz aus kompromittierten Endgeräten ist kein solcher Apparat; die Regelhaftigkeit eines Programms ist keine organisatorische Struktur im Sinne der Rechtsprechung. Für die §§ 303a, 303b StGB bestätigt sich dieser Befund in besonderer Weise: Die automatisierte Ausführung einer Datenveränderung oder Computersabotage spricht nicht für mittelbare Täterschaft, sondern für eine präzise Bestimmung des tatbestandlichen Kerngeschehens und eine daran ausgerichtete Versuchsschwelle. Der Gesetzgeber hat im digitalen Bereich bewusst eigenständige Vorbereitungstatbestände geschaffen (§§ 202c, 303a Abs. 3, 303b Abs. 5 StGB); eine Umgehung dieser Systementscheidung über § 25 Abs. 1 Alt. 2 StGB wäre dogmatisch nicht zu rechtfertigen.

Im Ergebnis ist eine „Software-Mittäterschaft" oder „mittelbare Täterschaft durch Systeme" dogmatisch verzichtbar und systematisch riskant. Das Strafrecht verfügt mit der unmittelbaren Täterschaft über Werkzeuggebrauch, der objektiven Zurechnung, der Mittäterschaft und Teilnahme für arbeitsteilige Rollenbeiträge sowie den punktuellen Vorbereitungstatbeständen über ein hinreichend differenziertes Instrumentarium, das digitale Angriffsszenarien erfasst, ohne die personenbezogene Struktur des Beteiligungssystems aufzugeben.

Kriminalpolitisch ergibt sich aus der Untersuchung, dass das Beteiligungssystem des StGB auch im Zeitalter automatisierter Angriffstechniken keiner strukturellen Erweiterung bedarf. Die Begrenzung der mittelbaren Täterschaft auf personale Vermittlung ist kein dogmatischer Formalismus, sondern rechtsstaatliche Notwendigkeit, die das Bestimmtheitsgebot und die schuldangemessene Individualisierung strafrechtlicher Verantwortung sichert. Wo kriminalpolitischer Handlungsbedarf besteht, ist er auf der Ebene deliktsspezifischer Vorbereitungstatbestände und forensischer Ermittlungskapazitäten – nicht aber durch eine Ausdehnung des Täterbegriffs – zu adressieren.