Bundeskriminalamt

KRIMINALISTISCHES INSTITUT

Aktuelles aus der kriminalistisch-kriminologischen Forschung

MONITORINGBERICHT

Cybercrime im engeren Sinne – Phänomenologie und Handlungsansätze

Referat IZ 33
Matthias Rau, Nicola Frost, Heike Bruhn

2025
2

Vorbemerkung

Das Kriminalistische Institut ist die kriminalistisch-kriminologische Forschungseinrichtung des Bundeskriminalamtes. Wissenschaftlerinnen und Wissenschaftler arbeiten gemeinsam mit Kriminalbeamtinnen und Kriminalbeamten daran, das Wissen über Ausmaß, Entstehungsgründe und Tatbegehungsformen von Kriminalität zu vertiefen.

Das Format „Aktuelles aus der kriminalistisch-kriminologischen Forschung“ (KKF-Aktuell) dient dazu, die Arbeitsergebnisse des Kriminalistischen Instituts zeitnah und bedarfsträgerorientiert für die polizeiliche Praxis nutzbar zu machen. Die Inhalte sollen dazu beitragen, die Erkenntnisbasis für die Entwicklung und Fortschreibung kriminalstrategischer und kriminalpräventiver Konzepte und Maßnahmen zu verbreitern und empirisch zu untermauern.

Forschungsberichte geben die Ergebnisse und polizeifachliche Relevanz eigener Studien des Kriminalistischen Instituts wieder. Monitoringberichte hingegen enthalten die wesentlichen Ergebnisse externer Studien zu einem polizeilich relevanten Themenfeld und bewerten deren polizeifachliche Relevanz.

Der vorliegende Bericht entstand mit Unterstützung der Abteilungen Cybercrime (CC) und Staatsschutz (ST) sowie des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und des Bundesamtes für Justiz (BfJ).

Inhaltsverzeichnis

Wesentliche Ergebnisse

- Die Bedrohung durch *Cybercrime im engeren Sinne* (i. e. S.) hat sich zu einer der vordringlichsten Herausforderungen in der IT-Sicherheitslandschaft entwickelt. Unter Cybercrime i. e. S. versteht das BKA Delikte, die sich unmittelbar gegen die Integrität und Verfügbarkeit des Internets und anderer Datennetze richten. Hierzu gehören das unbefugte Eindringen in fremde Netzwerke, das Ausspähen und Abfangen von Daten, oder Angriffe durch Schadsoftwares, die auf die Zerstörung oder Funktionsbeeinträchtigung von IT-Systemen abzielen. Phänomenologisch zählen zu Cybercrime i. e. S. unter anderem *Ransomware-Angriffe*, der *Missbrauch digitaler Identitätsdaten*, *Denial of Service-Angriffe* (DDoS) und *Cybercrime as a Service* (CaaS).
- Innerhalb der *Polizeilichen Kriminalstatistik* (PKS) werden Straftaten der Cybercrime (unter anderem) mit dem PKS-Summenschlüssel 897000 ausgewiesen. Für das Jahr 2024 wurden 131.391 Fälle (Inlandstaten) dokumentiert, von denen 31,9 % aufgeklärt werden konnten. Insgesamt wurden 30.669 tatverdächtige Personen ermittelt.
- Den seit 2021 in der PKS rückläufigen Fallzahlen der Inlandstaten stehen in den zurückliegenden Jahren fortlaufend *steigende Zahlen der Auslandstaten* gegenüber – sie stiegen zuletzt auf 201.877 Fälle im Jahr 2024. Bei diesen halten sich die tatverdächtigen Personen bei Tatbegehung nicht in Deutschland auf, der Schaden tritt jedoch in Deutschland ein.
- Die Höhe der *finanziellen Schäden*, die durch Cybercrimestraftaten entstanden sind, wird in der PKS nicht vollständig erfasst, einerseits aufgrund der bestehenden Erfassungsrichtlinien der PKS und andererseits auch, weil sich solche Schäden – obwohl erheblich – für die Polizei nur mit unverhältnismäßigem Aufwand und unter Rückgriff auf zahlreiche Annahmen schätzen lassen würden. Näherungen zu Schadenssummen lassen sich aus Berichten der Wirtschaft entnehmen. So stieg den regelmäßigen Wirtschaftsschutzberichten von Bitkom zufolge der ermittelte Schaden in Unternehmen im Zusammenhang mit Diebstahl, Industriespionage oder Sabotage ab dem Jahr 2017 auf eine Gesamtschadenssumme von zuletzt (2024) ca. 267 Mrd. Euro.[1] Zwei Drittel – ca. 179 Mrd. Euro – entfielen davon auf Cyberattacken.
- Zu den direkten finanziellen Verlusten durch Betrug, Erpressung oder Diebstahl von geistigem Eigentum und Daten werden öffentliche Institutionen, Unternehmen und die Gesellschaft durch *weitere Schäden* und Folgen belastet. Zu diesen zählen Investitionen in die Wiederherstellung betroffener Systeme, aber auch die Gefährdung der Gesundheit von Menschen, wenn etwa Gesundheitseinrichtungen angegriffen werden, oder immaterielle bzw. soziale Schäden wie der Verlust des Kundenvertrauens oder Verunsicherung in der Bevölkerung.
- In diesem Sinne sollte *Cybersicherheit* nicht nur als technische, sondern als *gesamtgesellschaftliche* Aufgabe verstanden werden. Die Aspekte Bildung und Sensibilisierung sind in der Prävention von Cybercrime i. e. S. von erheblicher Bedeutung. Indem Bürgerinnen und Bürger, Unternehmen und Organisationen über die Risiken aufgeklärt und in den effektiven Schutz ihrer Daten und Systeme eingebunden werden, kann die Resilienz gegenüber Cyberangriffen erhöht werden.

[1] *Bitkom e. V.*, 2024, 4.

Wesentliche Ergebnisse

- Die Förderung von Forschung und Entwicklung im Bereich der Cybersicherheitstechnologien ist entscheidend, um innovative Lösungen zu entwickeln. Mit Blick auf die Zukunft könnte der Einsatz von *Künstlicher Intelligenz* (KI) durch Cyberkriminelle einen Wendepunkt in der Evolution von Cyberangriffen darstellen, indem KI die Effizienz und die Reichweite cyberkrimineller Aktivitäten erweitert.[2] „KI-Modelle sind prinzipiell in der Lage, Schadsoftware zu programmieren, auf Fehler zu prüfen und ggf. auszubessern."[3]
- Auf der anderen Seite bietet *KI* das Potenzial, die *Bekämpfung von Cyberkriminalität voranzutreiben*, Schwachstellen aufzudecken oder Softwareentwicklerinnen und -entwicklern – beispielsweise durch die Analyse automatisierter Code-Bestandteile – zu unterstützen.[4]
- Cybercrime i. e. S. erfolgreich zu bekämpfen, erfordert ein koordiniertes Vorgehen, das technische Sicherheitsmaßnahmen mit rechtlichen Rahmenbedingungen und der aktiven Einbindung der gesamten Gesellschaft zusammenführt.

[2] Vgl. *Europol* 2025, 21.
[3] *BKA*, 2024a, 14.
[4] *AISEC*, 2023.

1 Einleitung und Begriffsbestimmungen

„Die Etablierung des Internets als sozialer Raum stellte die größte Umwälzung menschlicher Kommunikations- und Interaktionsformen der letzten Jahrzehnte dar.“[5] Die Digitalisierung hat das Alltags- und Wirtschaftsleben in den letzten Jahrzehnten grundlegend verändert und damit auch neue Tatgelegenheiten im digitalen Raum geschaffen.[6] Entsprechend steigen die qualitative und quantitative *Bedrohungslage* durch Cyberangriffe sowie die fortschreitende *Professionalisierung* von Cyberkriminellen in Deutschland seither kontinuierlich an.[7] Die Digitalisierungswelle, weiter beschleunigt durch die COVID-19-Pandemie, hat einen signifikanten Einfluss auf die Zunahme von Cybercrimedelikten und entsprechenden Angriffen. Die Verfügbarkeit von Künstlicher Intelligenz (KI) für viele Akteurinnen und Akteure und die damit verbundene Möglichkeit, generative KI-Tools für verschiedene Cybercrime-as-a-Service-Angebote nutzbar zu machen, könnten die bisherigen Entwicklungen verstärken.[8] Der vorliegende Monitoringbericht beleuchtet daher bisherige Entwicklungen und stellt Erkenntnisse zu zentralen Phänomenen der Cybercrime im engeren Sinne vor. Des Weiteren werden ätiologische Aspekte behandelt und präventive sowie repressive Ansatzpunkte eruiert.

Die wissenschaftlichen Bemühungen, eine einheitliche Definition für den Begriff Cybercrime zu finden, sind vielfältig. „Im Fall des Begriffs ‚Cybercrime‘ spannt sich der Bogen der Definitionen von Technik-, Rechts- und Wirtschaftswissenschaft bis hin zur Kriminologie, Psychologie und Soziologie. Diese Disziplinen haben sich übergreifend nicht auf einen einheitlichen Begriff verständigt, sodass unter dem Begriff ‚Cybercrime‘ maximal von einer Phänomenologie und nicht von einer Definition gesprochen werden kann.“[9] Das *BKA* unterscheidet definitorisch die Begriffe Cybercrime im engeren Sinne (i. e. S.) und Cybercrime im weiteren Sinne (i. w. S.):

- *Cybercrime i. e. S.* bezieht sich auf Delikte, die sich unmittelbar gegen die Integrität und Verfügbarkeit des Internets und anderer Datennetze richten. Hierzu gehören das unbefugte Eindringen in fremde Netzwerke, das Ausspähen und Abfangen von Daten, oder Angriffe durch Schadsoftwares, die auf die Zerstörung oder Funktionsbeeinträchtigung von IT-Systemen abzielen.
- Im Gegensatz dazu umfasst *Cybercrime i. w. S. Straftaten*, die mittels der Informationstechnik ausgeführt werden, wie Internetbetrug, Urheberrechtsverletzungen und Vertrieb illegaler Güter sowie Dienstleistungen über das Internet.[10]

Dem Bericht liegt die Definition des BKA zu Cybercrime i. e. S. zugrunde. Soweit an einzelnen Stellen bei Aussagen oder der Darstellung von Befunden von der Definition aus inhaltlichen Gründen abgewichen wird, sind diese sprachlich benannt.

Die COVID-19-Pandemie hat durch die Umstellung vieler Arbeitsplätze auf das Homeoffice und die vermehrte Nutzung digitaler Dienste für Freizeit und Onlineeinkäufe die Angriffsfläche für Cyberkriminelle erweitert. Dies hat zu einem erhöhten Aufkommen von Cybercrimedelikten geführt; insbesondere einem deutlichen Anstieg von Phishing-Angriffen. Eine ständige Anpassung präventiver Maßnahmen und Sensibilisierung der Bevölkerung ist daher erforderlich.[11] Ergänzend weisen

---

5 *Rettenberger/Leuschner* in: FPPK, 2020, 242.

6 Vgl. hierzu etwa *Beisch/Schäfer* in: Media Perspektiven, 2020; BMI/BMJV, 2021, 119; *Rüdiger/Bayerl* in: *Rüdiger/Bayerl*, 2020, 3.

7 *BKA*, 2023a, 4.

8 Vgl. hierzu *Europol*, 2025, 21; *BKA*, 2024a, 14.

9 *Huber*, 2019, 24.

10 *BKA*, o. J.

11 *BKA*, 2023a, 11 f.

Berichte des *Bundesamtes für Sicherheit in der Informationstechnik* (BSI)[12] und Studien führender Cybersecurity-Unternehmen, wie beispielsweise Veritas[13] und SoSafe[14], darauf hin, dass auch die Anzahl von Ransomware-Attacken und Identitätsdiebstählen während der Pandemie zugenommen haben.

Um die verschiedenen Formen von Cybercrime i. e. S. zu verstehen, ist eine detaillierte Betrachtung spezifischer Phänomene hilfreich. Diese Phänomene, die ein breites Spektrum von Methoden und Zielen abdecken, verdeutlichen die Vielfalt und die technischen Fähigkeiten Cyberkrimineller. Nachfolgend wird eine Auswahl aktuell besonders relevanter Cybercrimedelikte kurz erläutert:

- *Ransomware* ist eine Form der Malware[15], die Daten auf dem Computer des Opfers verschlüsselt bzw. unzugänglich macht. Im Anschluss fordern die Tatausübenden ein Lösegeld für die Entschlüsselung.[16] Bei einer erweiterten Variante – der sogenannten *Double Extortion* – werden die Daten vor der Verschlüsselung entwendet. Sollte das Opfer kein Lösegeld zahlen, so die Drohung, würden die gestohlenen Informationen veröffentlicht oder an Dritte zu verkauft.
- Beim *Diebstahl digitaler Identitäten* werden persönliche Daten illegal erworben, um beispielsweise Betrug oder Identitätsmissbrauch zu betreiben.[17] „Fremde missbrauchen die Identitäten von [Verbraucherinnen und Verbrauchern] in diversen Bereichen. Mithilfe der gestohlenen Daten werden im Internet kostenpflichtige Abos abgeschlossen, Nutzerkonten [sic] eingerichtet und Waren bestellt“[18], so schreibt die Verbraucherzentrale auf ihrer Internetseite.
- *DDoS-Attacken* (Distributed Denial of Service) überlasten gezielt die Server und Infrastruktur einer Webseite oder eines Netzwerkdienstes mit einer Flut von Anfragen, was zur Nichtverfügbarkeit des Dienstes führt.[19]
- Im Rahmen von *Cybercrime as a Service* (CaaS) bieten Kriminelle Dienstleistungen, wie das Mieten von Botnetzen für DDoS-Angriffe oder das Bereitstellen von Ransomware, im Austausch gegen Bezahlung an.[20]
- *Cyberspionage* bezieht sich auf das Ausspähen von Daten, oft zu politischen oder wirtschaftlichen Zwecken.[21] Ausländische Nachrichtendienste sind in Deutschland unvermindert aktiv. In ihrem Bestreben, möglichst umfassend Informationen aus den Bereichen Politik, Wirtschaft, Militär sowie zu sich hier aufhaltenden Oppositionellen zu erlangen, greifen sie in jüngster Zeit nicht mehr allein auf hinlänglich bekannte Begehungsweisen, wie z. B. auf offene Informationsbeschaffung, Einschleusung von Agenten oder technische Lauschangriffe, zurück. Ergänzend gewinnt seit geraumer Zeit die Informationsbeschaffung auf digitalem Weg bzw. durch technisch hochkomplexe elektronische Angriffe (Cyberspionage/-sabotage) für fremde Staaten an Bedeutung. „Im Bereich der Cyberspionage

12 *BSI*, 2023, 55.
13 *Veritas*, 2023, 3.
14 *SoSafe*, 2024, 11 f.
15 Malware „bezeichnet Software, die mit dem Ziel entwickelt wurde, unerwünschte und meist schädliche Funktionen auf einem IT-System auszuführen“ – *BSI*, 2024b.
16 *BSI*, 2023, 91.
17 *BSI*, 2023, 51.
18 *Verbraucherzentrale e. V.*, 2023.
19 *BSI*, 2023, 89.
20 *BSI*, 2023, 89.
21 *BSI*, 2023, 25.

dient die eingesetzte und oftmals modular aufgebaute Schadsoftware in erster Linie der Datenausspähung."[22] Da es sich bei dem Kreis der Täterinnen und Täter um staatlich/nachrichtendienstlich gesteuerte Akteure handelt, die mit entsprechend hohen finanziellen sowie personellen Mitteln ausgestattet sind und über einen qualifizierten technischen Sachverstand verfügen, zeigt sich die eingesetzte Malware zumeist technisch weit entwickelt und auf das konkrete Ziel zugeschnitten. Eine Zuordnung der Software zu einer nachrichtendienstlichen Kampagne und daraus resultierend einem angreifenden Staat ist daher erheblich erschwert. Ziele und auch angegriffene Bereiche der klassischen Spionage und der Cyberspionage sind identisch, es unterscheidet sich nur der Weg bzw. die Art der Informationsbeschaffung. Sofern diese Fälle bekannt werden, erfahren sie in der Regel in der Öffentlichkeit, den Medien und der Politik große Aufmerksamkeit.

2 Ausprägung, Entwicklung und Strafverfolgung von Cybercrime im engeren Sinne

2.1 Polizeiliches Hellfeld

Das nachfolgende Schaubild 1 zeigt die erfassten und aufgeklärten Fälle von *Cybercrime in Deutschland* für den Zeitraum von 2015 bis 2024, kodiert unter dem PKS-Summenschlüssel 897000. Die Anzahl der erfassten Fälle von Cybercrime ist seit 2015 bzw. 2016[23] bis zu einem Maximalwert im Jahr 2021 gestiegen. Seitdem sind die Zahlen in der PKS-Inland wieder rückläufig. Dieser Rückgang nach 2021 kann verschiedene Ursachen haben – zuvorderst ist „zu berücksichtigen, dass diese Fallzahlen … ausschließlich Taten umfassen, bei denen mindestens eine tatverdächtige Person im Inland gehandelt hat. Fälle, bei denen zwar Schäden in Deutschland verursacht werden, aber der Handlungsort der oder des Tatverdächtigen im Ausland liegt oder unbekannt ist (sogenannte Auslandstaten – welche insbesondere im Bereich Cybercrime eine überdurchschnittliche Relevanz aufweisen)" sind darin nicht enthalten.[24] Weitere denkbare Gründe für einen Rückgang der Inlandstaten im Hellfeld sind Erfolge der verstärkten Anstrengungen zur Prävention von Cybercrime, verbesserte Sicherheitstechnologien oder effektivere Strafverfolgungsmaßnahmen. Grundsätzlich kämen auch Verschiebungen zwischen Hellfeld und Dunkelfeld in Betracht.

Die PKS-Inland hat also „nur eine begrenzte Aussagekraft, da vielfach das Agieren der [Cybertäterinnen und] Cybertäter nicht im Inland verortet werden kann. Die Auslandstaten, bei denen sich die [Täterinnen und] Täter nicht in Deutschland aufhalten oder deren Aufenthaltsort unbekannt ist, geben hier ein realistischeres Bild wieder."[25] Seit dem Jahr 2020 werden Straftaten, die im Ausland (oder unbekanntem Tatort) begangen wurden und in Deutschland ihren Erfolgsort haben, in einem an die PKS-Inland angelehnten System erfasst.[26] Nach einer Pilot-/Erprobungsphase und

---

22 *Münch*, 2020, 7

23 Der starke Anstieg von 2015 zu 2016 lässt sich unter anderem auf die Zuordnungsumstellung im Bereich Computerbetrug zurückführen. Seit 2016 konnten Delikte, die unter (allgemeiner) Betrug fielen, eindeutiger zugeordnet werden. Computerbetrug macht fast drei Viertel aller Cybercrime-Straftaten aus, somit hat die neue Zuordnungsmöglichkeiten einen erheblichen Einfluss – *BKA*, 2017, 5.

24 *BMI*, 2024a, 27.

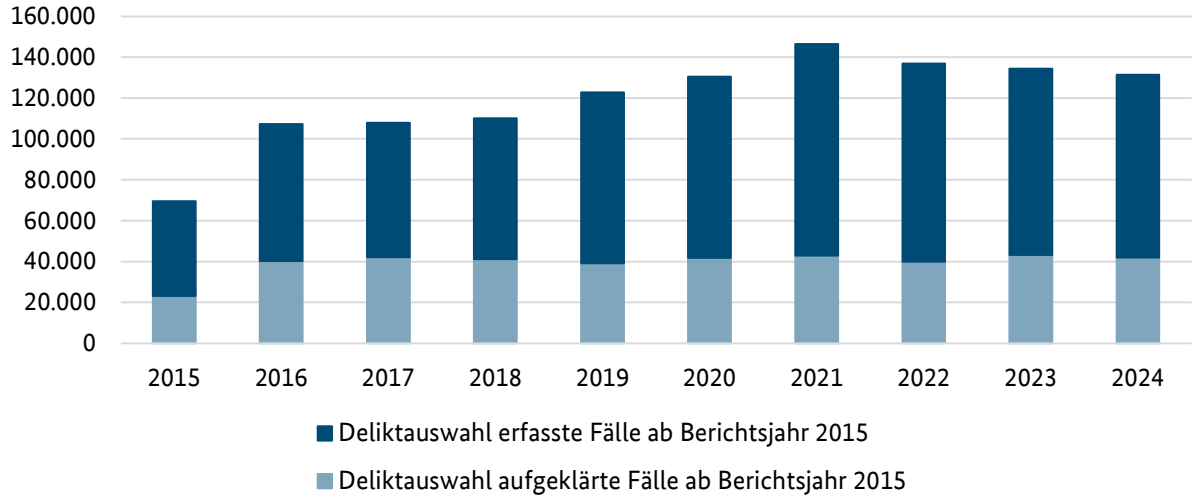
25 *BKA*, 2024a, 9.

26 *BMI*, 2025, 6.

Anpassungen liegen ab dem Berichtsjahr 2024 valide Daten der PKS-Ausland vor.[27] Demnach ist die Zahl der *Auslandstaten* im Bereich Cybercrime in den letzten Jahren fortlaufend gestiegen auf zuletzt 201.877 Fälle.[28]

Im Berichtsjahr 2024 wurden demgegenüber insgesamt 131.391 Inlandstaten erfasst, was im Vergleich zum Vorjahr eine Abnahme um 2,2 % darstellt. Bei der Aufklärungsquote von Cybercrime (31,9 % in 2024) zeigt sich ein Rückgang im Vergleich zum Vorjahr um knapp 0,3 Prozentpunkte.

Schaubild 1: Erfasste und aufgeklärte Fälle von Cybercrime 2015 – 2024[29]



Quelle: PKS, Summenschlüssel 897000, eigene Auswertung.

Im Vergleich zu anderen Deliktsbereichen zeigt sich, dass die Aufklärung von Cybercrime eine besondere Herausforderung für die Strafverfolgungsbehörden darstellt. Im Allgemeinen variieren Kriminalitätsraten aufgrund verschiedener Faktoren wie Demografie, sozioökonomische Bedingungen und polizeiliche Präsenz. Im Phänomen Cybercrime wirken sich zudem die technische Komponente sowie die globale Reichweite besonders intensiv aus. Die Täterinnen und Täter agieren oft anonym und international, was die Ermittlungen und die strafrechtliche Verfolgung deutlich erschwert.

---

27 *BMI*, 2025, 6.

28 *BMI*, 2025, 33.

29 Für die Berechnung der Fallzahlen des PKS-Summenschlüssels Cybercrime bis 2020 waren Delikte der Schlüssel 715100 und 715200 zu berücksichtigen. Aus diesen Schlüsseln sind in den Fallzahlen folgende Werte enthalten – erfasste Fälle: für 2015 *n* = 485; 2016 *n* = 473; 2017 *n* = 590; 2018 *n* = 396; 2019 *n* = 206; 2020 *n* = 134 davon aufgeklärte Fälle für 2013 *n* = 615; 2014 *n* = 283; 2015 *n* = 458; 2017 *n* = 498; 2018 *n* = 366; 2019 *n* = 189; 2020 *n* = 115.

Tabelle **1** zeigt auf der nachfolgenden Seite eine Auflistung von Fällen von Cybercrime im Jahr 2024 in Deutschland, kategorisiert nach verschiedenen Straftatbeständen. Es werden die Anzahl der erfassten Fälle und die zugehörige Aufklärungsquote dargestellt. Die Aufklärungsquoten variieren stark, je nach Deliktstyp.

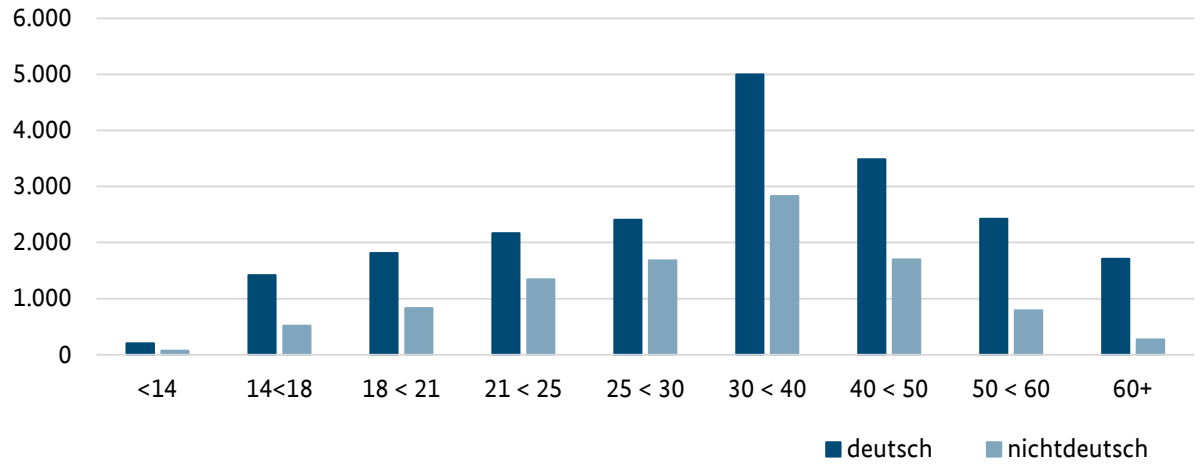
Tabelle 1: Fälle von Cybercrime 2024 (PKS-Inland)

Schlüssel	Straftat	Anzahl erfasste Fälle	Aufklärungsquote
897000	**Cybercrime**	**131.391**	**31,9 %**
	Darunter:		
	543000 Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei Datenverarbeitung §§ 269, 270 StGB	10.616	41,6 %
	674200 Datenveränderung, Computersabotage §§ 303a, 303b StGB	2.493	27,6 %
	678000 Ausspähen, Abfangen von Daten einschl. Vorbereitungshandlungen gemäß §§ 202a, 202b, 202c StGB	10.325	24,9 %
	897100 Computerbetrug § 263a StGB	107.957	31,7 %
	Darunter:		
	511120 Betrügerisches Erlangen von Kfz § 263a StGB	104	78,8 %
	511212 Weitere Arten des Warenkreditbetruges § 263a StGB	24.883	38,7 %
	516300 Computerbetrug mittels rechtswidrig erlangter Zahlungskarten mit PIN § 263a StGB	23.905	29,0 %
	516520 Computerbetrug mittels rechtswidrig erlangter Daten von Zahlungskarten § 263a StGB	23.601	18,0 %
	516920 Computerbetrug mittels rechtswidrig erlangter sonstiger unbarer Zahlungsmittel § 263a StGB	12.187	26,2 %
	517220 Leistungskreditbetrug § 263a StGB	3.582	45,3 %
	517500 Computerbetrug (sonstiger) § 263a StGB (soweit nicht unter den Schlüsseln 511120, 511212, 516300, 516520, 516920, 517220, 517900, 518112 bzw. 518302 zu erfassen)	17.548	43,6 %
	517900 Missbräuchliche Nutzung von Telekommunikationsdiensten § 263a StGB	203	52,7 %
	518112 Abrechnungsbetrug im Gesundheitswesen § 263a StGB	47	87,2 %
	518302 Überweisungsbetrug § 263a StGB	1.897	36,9 %
620017	Betreiben krimineller Handelsplattformen im Internet §127 StGB	92	12,0 %

Quelle: PKS, eigene Auswertung.

Im Jahr 2024 wurden insgesamt 30.669 tatverdächtige Personen (PKS-Inland) im Bereich Cybercrime ermittelt.[30] In der Analyse der Tatverdächtigen von Cybercrime in Deutschland zeigen sich demografische Unterschiede in Bezug auf Alter, Herkunft (siehe Schaubild 2) und Geschlecht. In allen Altersgruppen sind männliche Tatverdächtige häufiger vertreten als weibliche, was auch für die allgemeine Kriminalitätsverteilung in Deutschland gilt.[31] Die Gruppe der 30- bis unter 40-jährigen weist in Bezug auf Cybercrime im Jahr 2024 die höchste Anzahl an Tatverdächtigen auf. Der höhere Anteil von Männern könnte auf soziale und/oder psychologische Faktoren[32] zurückzuführen sein – denkbar wäre auch eine stärkere Affinität zu digitalen Technologien.

Schaubild 2: Tatverdächtige von Cybercrime gemäß PKS-Summenschlüssel 897000 nach Alter und Staatsangehörigkeit (deutsch/nichtdeutsch) für das Jahr 2024 (PKS-Inland)



Quelle: PKS, eigene Auswertung.

Der Anteil der Nichtdeutschen an allen Tatverdächtigen betrug hier im Jahr 2024 32,7 % (2023: 28,5 %). Die Verteilung der Tatverdächtigen fällt über die Alterskategorien hinweg bei Deutschen und Nichtdeutschen ähnlich aus; so sind beispielsweise bei den Nichtdeutschen ebenfalls Personen im Alter von 30 bis unter 40 Jahren am häufigsten vertreten. Grundsätzlich ist zu bedenken, dass Cybercrimedelikte in besonderem Maß staatenübergreifend vorkommen. Dementsprechend wirken viele ausländische Tatausübende, z. T. von ausländischen Nachrichtendiensten gelenkt und/oder geduldet, aus dem Ausland auf Ziele in Deutschland ein.[33] Die Anzahl der in der PKS-Ausland erfassten Tatverdächtigen lag im Berichtsjahr 2024 vor dem Hintergrund einer niedrigen Aufklärungsquote (2,2 %) bei 4.563 Personen.[34]

Cyberspionage

Im Rahmen der kriminalpolizeilichen Bearbeitung des Phänomens der Cyberspionage liegen dem BKA im Bereich des Hellfeldes valide Zahlen im Zeitraum zwischen 2014 und 2023 vor. Einen Überblick zu den Ermittlungsverfahren bietet Tabelle 2.
Politisch motivierte Cybercrime i. e. S., außerhalb der nachrichtendienstlich/staatlich gesteuerten Cybercrime, ist ein Phänomen, welches bundesweit in den letzten Jahren nur im sehr niedrigen zweistelligen Bereich aufgetreten ist. Im Rahmen der Kriminalitätsbekämpfung wird dem

30 *BMI*, 2025, 32.
31 Vgl. *Meier*, 2021, 138 f.
32 Vgl. *Neubacher*, 2023, 88 ff.
33 *BKA*, 2019, 48; 2022, 31.
34 *BMI*, 2025, 33.

Phänomen aktuell eine geringere Bedeutung zugemessen als der politisch motivierten Cybercrime i. w. S. (z. B. Hasskriminalität im Internet).

Tabelle 2: Ermittlungsverfahren Cyberspionage

	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023
Ermittlungs-verfahren BKA	3	6	4	6	5	4	4	7	9	9
Ermittlungsver-fahren Land	-	-	-	2	4	4	1	1	1	1
Gesamt	3	6	4	8	9	8	5	8	10	10

Quelle: BKA, eigene Auswertung.

2.2 Dunkelfeld

Die Bekämpfung von Cyberkriminalität in Deutschland steht vor erheblichen Herausforderungen, da das Kriminalitätsphänomen nicht nur technisch schwer zu bearbeiten, sondern auch kriminalstatistisch kaum zu fassen ist. Die PKS erfasst Straftaten nach Abschluss von polizeilichen Ermittlungen und auch die Erkenntnismöglichkeiten der Strafverfolgungs- und Strafvollzugsstatistik sind auf das Hellfeld und die im Strafgesetzbuch vorhandenen Straftatbestände begrenzt. Im Bereich der *Cyberkriminalität* bleibt der *ganz überwiegende Teil der Delikte* allerdings *unentdeckt* oder wird aus ganz unterschiedlichen Gründen nicht gemeldet.[35]

In der gemeinsamen Dunkelfeldbefragung des BKA und der Polizeien der Länder, SKiD 2020[36], wurden sowohl Opfererfahrungen abgefragt, die dem Bereich Cybercrime i. e. S. als auch solche, die dem Bereich Cybercrime i. w. S. zuzuordnen sind. Erhoben wurden folgende Delikte unter der Beschreibung „Cyberkriminalität gesamt (ohne Gewalt)“:

- Infizierung mit Computerviren,
- Cyberangriff auf das Online-Banking,
- Missbrauch persönlicher Daten bei Nutzung des Internets,
- Waren- oder Dienstleistungsbetrug im Internet,
- Sonstiger Betrug im Internet.[37]

Aufgrund des thematischen Bezugs werden die beiden erstgenannten Delikte hier näher betrachtet. Von einer Infizierung ihrer Systeme mit Computerviren waren innerhalb der Wohnbevölkerung ab 16 Jahren in Privathaushalten in den letzten zwölf Monate vor der Befragung 3,4 % betroffen. Einen Cyberangriff auf das Online-Banking erlitten 2,0 %. Bei beiden Delikten bestehen keine statistisch signifikanten Unterschiede zwischen verschiedenen Altersgruppen; allerdings waren Männer bei beiden Delikten statistisch signifikant häufiger betroffen.[38] Auch hinsichtlich der Inzidenzraten,

---

35 *BKA*, 2023a, i.

36 Zur Teilnahme an der Befragung waren ab Anfang November 2020 n = 122.667 Bürgerinnen und Bürger eingeladen, von denen sich n = 46.813 Personen an der Befragung beteiligten. Insgesamt waren n = 45.351 Interviews auswertbar – vgl. *Birkel* u. a., 2022, VI.

37 *Birkel* u. a., 2022, 15. Zusätzlich zu den fünf Delikten wurden für SKiD 2020 auch die Delikte *Gewaltandrohung im Internet* und *Beleidigung im Internet* erhoben. Für diese Beiden erfolgte eine Zuordnung zu den Gewaltdelikten unter der Kategorie *verbale Gewalt online*. Die Kategorie „Cyberkriminalität gesamt“ umfasst ausschließlich Eigentums- und Vermögensdelikte.

38 *Birkel* u. a., 2022, 24 u. 29.

berechnet pro 1.000 Einwohnerinnen und Einwohner, waren Männer statistisch signifikant häufiger betroffen. Bei der Infizierung mit Viren waren für die Computersysteme von Männern 77,5 Ereignisse pro 1.000 Einwohner zu verzeichnen, bei Frauen waren es 32,5 pro 1.000 Einwohnerinnen. Bei Cyberangriffen auf das Online-Banking lag die Inzidenzrate für Männer bei 34,1 und für Frauen bei 16,9.[39]

Die allermeisten dieser Straftaten verblieben im Dunkelfeld. Von den Cyberangriffen auf das Online-Banking wurden 23,7 % zur Anzeige gebracht. Die Anzeigequote für die Infizierung eines Systems mit Computerviren lag mit 11,6 % noch deutlich niedriger.[40] Über alle bei SKiD 2020 erfassten Cybercrimedelikte hinweg wurde etwa eine Straftat von fünf Straftaten angezeigt.[41] Die erhobenen Delikte sind dabei nicht direkt mit dem PKS-Summenschlüssel Cybercrime vergleichbar. Die Ergebnisse anderer Studien weisen aber ebenfalls auf ähnliche Dunkelziffern hin.[42] Bisher können auf Basis der SKiD-Studie noch keine Aussagen zur Veränderung des Dunkelfelds dahingehend getroffen werden, ob Veränderungen im Hellfeld auf tatsächliche Veränderungen des Fallaufkommens oder ein verändertes Anzeigeverhalten zurückzuführen sind.[43] Einen gewissen Aufschluss könnten zusätzliche Analysen von Daten der zweiten Erhebungswelle von SKiD – deren Kernbefunde im Laufe des Jahres 2025 vorliegen – bieten.

DREIßIGACKER U. A. berichten aus zwei Studien zu Cyberangriffen auf Unternehmen, dass von den befragten Firmen 88,1 % (Befragung I) bzw. 91,5 % (Befragung II) keine Anzeige bzgl. des schwerwiegendsten Vorfalls erstattet haben.[44] *Die empirischen Befunde zum Dunkelfeld unterstreichen die begrenzte Aussagekraft der Kriminalstatistiken und mahnen eine kritische Auseinandersetzung mit den bestehenden Dokumentationsmöglichkeiten und Bekämpfungsstrategien an.*

Ein wesentlicher Faktor für das ausgeprägte Dunkelfeld sind technische Sicherungseinrichtungen, die viele Cyberangriffe bereits im Versuchsstadium unterbinden.[45] Dies führt dazu, dass potenzielle Opfer von diesen Aktivitäten nichts bemerken. Obwohl dies ein Erfolg im Kampf gegen Cyberkriminalität ist, erschwert es gleichzeitig die Erfassung der tatsächlichen Anzahl von Angriffsversuchen. Darüber hinaus erkennen viele Opfer nicht, dass sie von Cyberkriminalität betroffen sind. Dies gilt insbesondere für den Diebstahl von Identitäten bei Online-Einkäufen oder den Missbrauch eigener Geräte, wie PCs oder Router, die als Teil eines Botnetzes[46] für DDoS-Angriffe verwendet werden. Dieser Mangel an Bewusstsein bzw. an Entdeckungsmöglichkeiten führt dazu, dass viele Vorfälle nicht gemeldet werden.

Viele Betroffene sehen zudem von einer Anzeige ab, wenn kein direkter finanzieller Schaden entstanden ist oder wenn dieser bereits von Dritten, wie z. B. Versicherungen, reguliert wurde. Insbesondere Unternehmen tendieren dazu, erkannte Straftaten nicht anzuzeigen, um ihre Reputation als sicherer und zuverlässiger Partner nicht zu gefährden.[47] Die Sorge um das Kundenvertrauen wiegt oft schwerer als das Bestreben, zur strafrechtlichen Verfolgung beizutragen. In Fällen von

---

39 *Birkel* u. a., 2022, 25.

40 *Birkel* u. a., 2022, 68.

41 *Birkel* u. a., 2022, 66.

42 *BMI*, 2024a, 27 mit Verweis auf *Dreißigacker* u. a., 2021, 86; *Riesner/Glaubitz*, 2020, 24. Zu den Befunden von *Dreißigacker* u. a., 2021 siehe unten.

43 *BMI*, 2024a, 27.

44 In der ersten Befragung gaben *N* = 1.726 Unternehmen, in der zweiten Befragung *N* = 279 Unternehmen Informationen zur Anzeigenerstattung bezogen auf den schwerwiegendsten Vorfall an – *Dreißigacker* u. a., 2021, 70 f.

45 *BKA*, 2021, 9.

46 Ein Botnetz ist ein Verbund von mit Schadsoftware infizierten, internetverbundenen Geräten – *BSI*, 2023, 88.

47 *BKA*, 2021, 9.

Erpressungen mittels Ransomware entscheiden sich Geschädigte oft nur dann für eine Anzeige, wenn trotz der Zahlung eines Lösegelds keine Entschlüsselung der betroffenen Systeme erfolgt.[48]

Zusätzlich zu diesen Faktoren erschwert die Komplexität und Dynamik der Cyberbedrohungen die Bekämpfung des Phänomens. Die rasante Entwicklung neuer Technologien führt zu immer ausgereifteren Angriffsmethoden, deren Erkennung und Bekämpfung selbst für Expertinnen und Experten eine Herausforderung darstellt. Der Mangel an Ressourcen und Know-how, insbesondere bei kleinen und mittleren Unternehmen (KMU), sowie psychologische Barrieren, wie Schamgefühl oder Angst vor Stigmatisierung, halten viele Opfer davon ab, Delikte zu melden. Die internationale Dimension vieler Cyberangriffe erschwert die Strafverfolgung zusätzlich und mindert die Wahrscheinlichkeit, dass Vorfälle gemeldet werden. Unklarheiten in den rechtlichen Rahmenbedingungen[49] sowie die Unterschätzung der Langzeitfolgen eines Cyberangriffs tragen ebenfalls dazu bei, dass das Dunkelfeld von Cyberkriminalität weiterhin groß bleibt.

Ein umfassendes Verständnis des Dunkelfelds, eine Erhöhung der Meldebereitschaft und die Intensivierung der Zusammenarbeit zwischen den Strafverfolgungsbehörden, der Wirtschaft und der Zivilgesellschaft sind unerlässlich, um effektiv gegen Cyberkriminalität vorzugehen. Es bedarf also gezielter Präventionsmaßnahmen, der Verbesserung technischer und rechtlicher Rahmenbedingungen sowie der Förderung von Aufklärung und Bildung, um das Dunkelfeld zu reduzieren und die Cybersicherheit zu stärken.[50]

2.3 Internationale Perspektive

Cybertäterinnen und -täter agieren global. Zur besseren Abbildung der Cyberkriminalität wurde daher zum 01. Januar 2020 die Erfassung von Auslandstaten in der PKS eingeführt. Darunter werden Straftaten verstanden, bei denen der Schaden in Deutschland entsteht, die dafür verantwortlichen Personen aber aus dem Ausland heraus handeln bzw. deren Aufenthaltsort nicht bekannt ist. Auf die Abbildung absoluter Fallzahlen wurde bis zum Berichtsjahr 2023 verzichtet, da es insbesondere zu Beginn der Erfassung noch zu Ungenauigkeiten kam. Die vorliegenden Daten zeigen, dass die Auslandstaten seit der erstmaligen Erfassung kontinuierlich anstiegen.[51] Es wurden weitere Maßnahmen zur Verbesserung der Datengrundlage eingeleitet, um zukünftig ein realistischeres Bild der Cyberkriminalitätslandschaft zu zeichnen.[52] Das im Laufe des Jahres 2025 erscheinende Bundeslagebild Cybercrime 2024 wird hierzu weitere Ausführungen bereithalten.

Der russische Angriffskrieg auf die Ukraine hat die Dynamik von Cyberkriminalität maßgeblich beeinflusst und das Bedrohungspotenzial im Cyberraum erhöht. Eine Folge des Konflikts im Cyberraum ist das Verschwimmen von staatlicher und finanziell motivierter Cyberkriminalität. Zuvor primär finanziell motivierte Akteure bezogen mit Ausbruch des Krieges vermehrt politisch Stellung und weiteten ihren Fokus auf ideologische Gegner aus. Dabei kann nicht ausgeschlossen werden, dass finanziell motivierte Täterinnen und Täter den Krieg und entsprechende ideologische Positionierungen als Vorwand nutzen, um sich selbst zu etablieren. Aktivitäten jener Akteure machen dabei häufig nicht an Ländergrenzen halt und können schnell Auswirkungen auf Unternehmen, kritische Infrastrukturen und staatliche Einrichtungen auch in nicht direkt am Krieg beteiligten Staaten haben.[53]

---

48 *BKA*, 2020a, 3.
49 *BKA*, 2023a, 30 f.
50 *BKA*, 2022, 37 f.
51 *BMI*, 2025, 33; *BKA*, 2024a, 8. Siehe hierzu auch oben, Kapitel 2.1.
52 *BKA*, 2023a, 6 ff.
53 *BKA*, 2023a, 22.

Trotz der bereits bei Kriegsbeginn errichteten Drohkulissen konnten in der Folge bisher – Stand März 2025 – keine schwerwiegenden Angriffe gegen deutsche Einrichtungen und Organisationen festgestellt werden. Angesichts der Aufrechterhaltung auch medial vermittelter Drohungen der russischen Regierung gegen Unterstützerstaaten der Ukraine besteht aber weiterhin ein hohes Eskalationspotential mit Blick auf die Sicherheitslage im Cyberraum. Insbesondere eine mögliche Ausweitung des Konfliktes auf weitere Staaten sowie die Realisierung einer Cyberoffensive, einschließlich Angriffe auf kritische Infrastrukturen und öffentliche Einrichtungen, bergen ein hohes Gefährdungspotential.[54]

„Die registrierten DDoS-Angriffe pro-russischer Aktivisten haben bisher wenig bis keinen bleibenden Schaden anrichten können. Da dies zum großen Teil auch an der gewählten Angriffsart DDoS liegt, sind die bisherigen Angriffe eher dem Bereich Propaganda zuzuordnen – mit dem Ziel, Verunsicherung zu stiften und das Vertrauen in den Staat zu untergraben."[55]

Das Unternehmen Recorded Future hebt hervor, dass der Krieg in der Ukraine das Phänomen Cyberkriminalität grundlegend verändert hat, indem er die Grenzen zwischen staatlich gesponserten Cyberaktivitäten und den anderweitigen – nicht staatlich motivierten – Aktivitäten der Kriminellen verschwimmen ließe.[56] Diese Entwicklungen verdeutlichen die Notwendigkeit einer fortgesetzten internationalen Kooperation und den Austausch von *Best Practices* zur Abwehr von Bedrohungen. Das vermehrte Aufkommen konkreter Cyberangriffe auf deutsche Unternehmen und staatliche Einrichtungen verdeutlicht die praktische Relevanz der internationalen Dimension von Cybercrime.[57] Die Analysen zeigen die Komplexität und die Auswirkungen dieser Angriffe auf die deutsche Wirtschaft und Gesellschaft.

Die internationale Kooperation zur Bekämpfung von Cybercrime umfasst spezifische Programme, Abkommen oder Initiativen, an denen Deutschland beteiligt ist. Diese Kooperationen innerhalb der Europäischen Union, mit NATO-Partnern oder durch globale Netzwerke wie Interpol sind entscheidend für die effektive Bekämpfung von Cyberkriminalität. Hierbei handelt es sich beispielsweise um das European Cybercrime Centre – EC3, die European Multidisciplinary Platform Against Criminal Threats (EMPACT-Cyber), die Counter Ransomware Initiative (CRI), Incident Response Teams der Bundeswehr sowie die Kampagne Cybercrime – #YouMayBeNext von Interpol.[58]

Zukünftige Herausforderungen im Bereich Cybercrime erfordern innovative Ansätze und Technologien, um Cyberbedrohungen wirksam zu begegnen. Die Entwicklung von KI in der Bedrohungserkennung und die Stärkung der Cybersicherheitskompetenzen sind zentral für die Zukunft der Cyberabwehr. Diese proaktiven Schritte Deutschlands und der internationalen Gemeinschaft sind entscheidend, um die Sicherheit im digitalen Raum zu gewährleisten und die Resilienz gegenüber Cyberbedrohungen zu stärken.

2.4 Schäden

Die Höhe der finanziellen Schäden, die durch Cybercrimestraftaten entstanden sind, wird in der PKS nicht vollständig erfasst, einerseits aufgrund der bestehenden Erfassungsrichtlinien der PKS und andererseits auch, weil sich solche Schäden – obwohl erheblich – für die Polizei nur mit unverhältnismäßigem Aufwand und unter Rückgriff auf zahlreiche Annahmen schätzen lassen würden. Der von der PKS erfasste Schaden mit Cyberbezug wird unter anderem für den PKS-Schlüssel

54 *BKA*, 2023a, 22.
55 *BSI*, 2023, 86.
56 *Recorded Future*, 2023, 2.
57 Siehe beispielweise Cyberangriffe auf ViaSat und Rosneft Deutschland GmbH – vgl. *BKA*, 2023a, 23.
58 *Europol*, 2024; 2022; *The White House*, 2023; *Bundeswehr*, o. J.; *Interpol*, o. J.

„Computerbetrug § 263a StGB“ ermittelt, welcher allerdings zu Cybercrimestraftaten i. w. S. zu zählen ist. Der zugehörige Schaden dieses Delikts wurde für das Jahr 2024 in der PKS-Inland auf 164,1 Mio. Euro[59] und in der PKS-Ausland auf 194 Mio. Euro[60] beziffert

Um sich an etwaige Schadenssummen anzunähern, wird im Folgenden auf Veröffentlichungen aus der Wirtschaft von Bitkom e. V., Coveware, Chainalysis und Sophos sowie einen Forschungsbericht zu Kosten und Schäden von Cyberkriminalität in Deutschland von WEBER zurückgegriffen.[61]

Den regelmäßigen Wirtschaftsschutzberichten von Bitkom zufolge stieg der ermittelte Schaden ab dem Jahr 2017 (vgl. hierzu Tabelle 3). Für das Jahr 2024 ergab sich eine Gesamtschadenssumme in Höhe von ca. 267 Mrd. Euro.[62] Schäden, die explizit durch Cyberangriffe entstanden sind, nahmen in diesem Jahr einen Anteil von 67 % an den Gesamtschäden ein, was etwa 178,6 Mrd. Euro entspricht.[63] Dieser Anteil betrug bei den 2023 veröffentlichten Gesamtschäden 72 % und in 2022 63 %.

Tabelle 3: Schadenssummen in Mrd. Euro, verursacht unter anderem durch Cybercrime

Schaden durch	2015	2017	2019	2021	2022	2023	2024
Ausfall, Diebstahl oder Schädigung von Informations- und Produktionssystemen oder Betriebsabläufen	7,2	5,3	13,5	61,9	41,5	35,0	54,4
Erpressung mit gestohlenen Daten oder verschlüsselten Daten	1,5	0,7	5,3	24,3	10,7	16,1	13,4
Datenschutzrechtliche Maßnahmen (z. B. Information von Kunden)	2,0	3,2	4,4	17,1	18,3	12,4	27,2
Geldabfluss durch Betrugsversuche	-	-	-	-	-	3,9	0,8
Patentrechtsverletzungen (auch schon vor der Anmeldung)	9,4	7,7	14,3	30,5	18,8	10,4	14,8
Umsatzeinbußen durch Verlust von Wettbewerbsvorteilen	6,4	8,6	11,1	29,0	41,5	21,5	11,2
Umsatzeinbußen durch nachgemachte Produkte (Plagiate)	11,5	3,5	11,1	22,7	21,1	15,3	39,2
Imageschaden bei Kunden oder Lieferanten/Negative Medienberichterstattung	5,9	7,7	9,3	12,3	23,6	35,3	20,2
Kosten für Ermittlungen und Ersatzmaßnahmen	-	10,6	18,3	13,3	10,1	25,2	32,2
Kosten für Rechtsstreitigkeiten	6,5	5,5	15,6	12,4	16,2	29,8	53,1
Höhere Mitarbeiterfluktuation/Abwerben von Mitarbeitern	0,9	2,2	-	-	-	-	-
Sonstige Schäden	0,1	< 0,1	< 0,1	0	0,9	1,1	0
Gesamtschaden pro Jahr	**51,2**	**54,8**	**102,9**	**223,5**	**202,7**	**205,9**	**266,6**

Quellen: *Bitkom e. V.*, 2021; 2022; 2023; 2024.
Anmerkung: Die angegebenen Jahreszahlen beziehen sich auf das Veröffentlichungsdatum des jeweiligen Berichts.

[59] *BKA*, 2025a. Im Jahr 2023 betrug der Schaden 166,8 Mio. Euro – vgl. *BKA*, 2024b.
[60] *BKA*, 2025b.
[61] *Weber*, 2024.
[62] *Bitkom e. V.*, 2024, 4.
[63] *Bitkom e. V.*, 2024, 13.

Schäden durch Ransomware-Zahlungen

Dem Cybersecurity Unternehmen Coveware zufolge geht die Zahlungsbereitschaft von durch Ransomware-Angriffe betroffenen Unternehmen fortlaufend zurück. Nach Einschätzung von Coveware versuchen Ransomware-Gruppierungen die daraus resultierenden finanziellen Einbußen durch höhere Lösegeldforderungen auszugleichen. So stellte das Unternehmen bei der Betrachtung der global gezahlten Lösegeldsummen fest, dass diese im vierten Quartal 2023 im Median bei 200.000 US-Dollar lagen.[64] Die Höhe geforderter Lösegeldsummen orientiert sich häufig an der Zahlungsfähigkeit eines betroffenen Unternehmens. Auch das Blockchain-Analyseunternehmen Chainalysis veröffentlicht Erkenntnisse zu den kriminellen Einnahmen durch Lösegeldzahlungen nach Ransomware-Angriffen. Die zuletzt abgebildeten fünf Jahre unterlagen hinsichtlich der dokumentierten Summen allerdings großen Schwankungen. Von 2019 über 2020 zu 2021 stiegen die Zahlungen an (von 220 Mio. auf 905 Mio. zu 983 Mio. US-Dollar), fielen im Jahr 2022 ab (auf 567 Mio. US-Dollar) und stiegen im Jahr 2023 wieder deutlich an – erstmals auf über eine Milliarde US-Dollar (1,1 Mrd.).[65]

Modell zur Systematisierung der Kosten und Schäden von WEBER

In dem von WEBER verfassten Forschungsbericht „Kosten und Schäden durch Cyber-Kriminalität in Deutschland“ wird auf Basis der Analyse wissenschaftlicher Literatur ein Modell entwickelt, das der Systematisierung von Kosten und Schäden durch Cyberkriminalität dienen soll. Im Rahmen dieses Modells werden die Schäden zunächst in zwei zentrale Kategorien eingeteilt: Die finanziell messbaren Schäden (Kosten) und die finanziell nicht messbaren oder nicht schätzbaren Schäden. Diese Einteilung erfolgt in Anlehnung an wissenschaftliche Studien und Modelle.[66]

Das Modell differenziert zudem hinsichtlich der Ebenen, auf denen die Schäden verursacht werden (Privatpersonen, Unternehmen, Staat)[67] sowie hinsichtlich des Zeitpunktes: Durch Präventionsbemühungen, als direkte Konsequenz der Straftat oder als Reaktion auf die Straftat.[68]

Tabelle 4: Modell zur Schätzung der Kosten (finanziell messbare Schäden)

	Präventionskosten	Kosten als direkte Konsequenz der Straftat	Kosten als Reaktion auf die Straftat
Privatpersonen	▪ Ausgaben für Sicherheitssysteme, Antiviren-Software auf privaten Geräten	▪ Verlust/Zerstörung von Eigentum	▪ Anwaltskosten, evtl. Gerichtskosten
Unternehmen	▪ IT-Personal ▪ Technische Schutzmaßnahmen (Cybersicherheit) ▪ Cyberversicherungen ▪ Mitarbeiter/innen-Schulungen	▪ Direkte Kosten durch Verlust/Zerstörung von Daten/ Infrastruktur/Hardware ▪ Produktivitätsverlust durch Störungen im Betriebsablauf	▪ Kosten für Ermittlungen und Ersatzmaßnahmen ▪ Kosten für Rechtsstreitigkeiten ▪ Zahlungen in Folge von Erpressung durch gestohlene/ verschlüsselte Daten

64 *Coveware*, 2024.
65 *Chainalysis*, 2024, 11. Die Daten von Chainalysis unterliegen retrograden Anpassungen.
66 *GAO*, 2017, 5 ff.; *Greenfield/Paoli*, 2013, 868 f.; *Paoli* u. a., 2018, 18.
67 Vgl. *GAO*, 2017; *Paoli* u. a., 2018.
68 *Weber*, 2024, 13 f. unter Bezugnahme auf *GAO*, 2017.

Staat und Gesellschaft	▪ Kosten für Kriminalpräventionsprogramme ▪ Staatliche Investitionen in Cybersicherheit (Staatliche Einrichtungen, Forschungsförderprogramme)	▪ Zerstörung staatlicher Infrastrukturen durch Cyberangriffe	▪ Polizei-/Ermittlungskosten ▪ Gerichtliche Kosten, Inhaftierungskosten

Quelle: *Weber*, 2024, 15, eigene Bearbeitung.
Anmerkung: Annäherung z. B. durch Erkenntnisse kommerzieller und wissenschaftlicher Studien.

Tabelle 5: Modell der finanziell nicht messbaren oder nicht schätzbaren Schäden

	Durch Präventionsbemühungen	Schäden als direkte Konsequenz der Straftat	Schäden als Reaktion auf die Straftat
Privatpersonen	▪ Vermeidungsverhalten (z. B. von Onlinediensten)	▪ psychische Auswirkungen auf das Opfer, Verlust von Lebensqualität	▪ Zeitaufwand/Stress durch Anzeige, ggf. Anklage, gesundheitliche Folgen, Folgen für Dritte (Familie…)
Unternehmen	▪ Verzicht auf Digitalisierungsschritte, damit Verzicht auf Effizienzsteigerung	▪ Imageschaden bei Bekanntwerden des Cyberangriffs	▪ Verlust von Kundschaft aufgrund von Imageschaden ▪ Minderung des Unternehmenswertes (z. B. durch reduziertes Wachstum)[69]
Staat und Gesellschaft	▪ Verzicht auf Einsatz an sich geeigneter Infrastrukturkomponenten, denen höhere Angreifbarkeit durch Cyberkriminalität zugeschrieben wird	▪ durch Cyberkriminalität erzwungenes Aussetzen staatlichen Handelns	▪ Verlust von Vertrauen in staatliche Institutionen (Sicherheitsbehörden, Verwaltungen) und Prozesse (Meinungsbildung, Wahlen)

Quelle: *Weber*, 2024, 16, eigene Bearbeitung.
Anmerkung: Annäherung z. B. durch qualitative Studien und/oder Expertinnen bzw. Experteninterviews.

Für den Themenbereich Kosten und Schäden durch Cyberkriminalität gibt es bislang in Deutschland nur wenige empirisch fundierte Studien, die zuverlässige Aussagen über die Kosten und Schäden von Privatpersonen, Unternehmen und Staat erlauben. Viele dieser Studien weisen methodische Unterschiede, wie etwa unterschiedliche Stichproben, oder andere methodische Schwierigkeiten auf, weshalb die Aussagen sich nur begrenzt verallgemeinern lassen.[70]

[69] „Hierbei handelt es sich um einen Schaden, der sich in der Theorie zwar prinzipiell in finanziellen Geldwerten messen lässt, aber faktisch unmöglich schätzbar ist. Da der Börsenwert eines Unternehmens von sehr vielen Faktoren beeinflusst wird und die Auswirkungen eines Cyberangriffs z. T. sehr stark verzögert auftreten können, lassen sich Veränderungen des Unternehmenswertes sehr schwer auf einzelne Angriffe zurückführen. Daher wird dieser Schadenspunkt hier als ‚nicht schätzbarer Schaden' mitaufgeführt" – *Weber*, 2024, 16.

[70] Vgl. weiterführend *Weber*, 2024, 17 ff.

Tabelle 6: Finanziell messbare Schäden (Kosten)

	Präventionskosten	Kosten als direkte Konsequenz der Straftat	Kosten als Reaktion auf die Straftat
Privatpersonen	▪ 259 Mio. Euro jährlich für Abonnements (Antivirenprogramme) ▪ ca. 675 Mio. Euro für Einmalzahlungen über mehrere Jahre (Antivirenprogramme)	▪ ca. 700 Mio. Euro ▪ Min. 56 Mio., Max. 5,6 Mrd.	▪ keine Datengrundlage
Unternehmen	▪ mind. 87 Mrd. Euro Personal ▪ mind. 1,4 Mrd. Euro IT-Sicherheitstechnik	▪ mind. 1,9 Mrd. – 2,65 Mrd. Euro ▪ mind. 500 Mio.	▪ ca. 30 – 80 % der Gesamtkosten[71]

Quelle: *Weber*, 2024, 20 und 31, eigene Bearbeitung.

„Für die Ebene Staat und Gesellschaft liegen bislang die wenigsten empirischen Daten vor, sodass eine Schätzung der Kosten hier nicht möglich erschien."[72] Für die Ebenen Privatpersonen und Unternehmen lässt sich jedoch festhalten, dass die Kosten als direkte Konsequenz und als Reaktion auf die Straftat auf insgesamt *rund 3,1 bis 3,7 Mrd. Euro pro Jahr* geschätzt werden können. In diesen Kosten sind nicht die Kosten inbegriffen, die durch Präventionsbemühungen entstehen. Diese dürften sich auf insgesamt etwa 89,3 Mrd. Euro belaufen, „wobei in dieser Schätzung die mit Abstand größte Kostenposition durch die geschätzten Personalausgaben von Unternehmen ... zustande kommt" (ca. 87 Mrd. Euro).[73] Die Kosten der Prävention übersteigen damit vermeintlich deutlich die direkten Folgekosten von Cyberangriffen oder diejenigen Kosten, die als Reaktion auf die Straftat anfallen. Diese Einschätzung teilten in den zurückliegenden Jahren z. T. auch Verantwortliche und Mitarbeitende in Unternehmen.[74] Ein Blick auf Tabelle 4 bis Tabelle 6 verdeutlicht jedoch: *Im Schadensfall dreht sich das Verhältnis für betroffene Personen bzw. Unternehmen ins Gegenteil und die messbaren bzw. nicht schätzbaren Schäden übersteigen die Kosten der Prävention bei weitem.*

Neben der monetären Dimension von Schäden beschreibt WEBER auch nicht finanziell messbare bzw. nicht schätzbare Schäden als Konsequenz von Cyberkriminalität. Demnach könne es auf individueller Ebene beispielsweise zu „psychischen sowie physischen Leiden der Betroffenen kommen sowie zu einem erheblichen Zeitaufwand und Stress, z. B. durch einen vorübergehend fehlenden Zugriff auf das persönliche Online-Banking."[75] Auf Unternehmensebene wären z. B. zunächst Image-Verluste denkbar, die in der Konsequenz ein mangelndes Vertrauen der Kundschaft und ggf. deren Verlust nach sich ziehen. Dies kann sich wiederum bis hin zur Minderung des Unternehmenswertes auswirken.[76]

---

71 Es liegen aus der Literatur kaum (gesondert ausgewiesene) Informationen zu der Kategorie „Kosten als Reaktion auf die Straftat" vor. Die hier bezifferte Spanne ergibt sich aus den Ergebnissen verschiedener Studien – vgl. *Weber*, 2024, 30. Die Prozentwerte sind daher nicht unmittelbar auf die (addierten) Werte der voranstehenden Spalten zu beziehen.

72 *Weber*, 2024, 37.

73 *Weber*, 2024, 37.

74 Vgl. exemplarisch *Hillebrand* u. a., 2017, 76 u. 81.

75 *Weber*, 2024, 38.

76 Vgl. *Weber*, 2024, 38.

3 Darstellung zentraler Phänomene

3.1 Ransomware

„Als Ransomware werden Schadprogramme bezeichnet, die den Zugriff auf Daten und Systeme einschränken oder verhindern (...).“[77] Dabei werden die komplette Festplatte, einzelne Partitionen oder gezielt bestimmte Dateiformate (z. B. .docx, .xlsx, .jpg, .jpeg) verschlüsselt. Für die Wiederherstellung wird meist ein Lösegeld gefordert.[78]

Es gibt zwei verschiedene Arten von Ransomware: Screenlocker und File-Encrypter. Screenlocker sperren den Bildschirm des Nutzenden und verhindern so den Zugriff auf das System, ohne die Festplatte zu verschlüsseln. Die bekanntesten Ausprägungen sind Schadprogramme, bei denen Namen und Logos von Sicherheitsbehörden missbraucht werden, um der kriminellen Zahlungsaufforderung einen offiziellen Charakter zu verleihen. File-Encrypter verschlüsseln Daten hingegen auf dem Computer und nehmen wichtige Dateien als „Geisel“. Die Daten werden auf den infizierten Endsystemen und aktuell auch mittels der mit dem Netzwerk verbundenen Systeme (Server, Dateiablagen etc.) verschlüsselt. Diese Variante ist gefährlicher, da die Verschlüsselungen nicht immer überwunden werden können und die Zahlung des Lösegelds häufig nicht zur Entschlüsselung führt.[79]

Die digitale Erpressung mittels Ransomware ist ein in Deutschland und auch international ein beständig und zahlreich auftretendes Phänomen.[80] Angriffe auf kritische Infrastrukturen (KRITIS), wie beispielsweise Versorgungsunternehmen (Strom, Wasser etc.), Krankenhäuser, die öffentliche Verwaltung oder internationale Lieferketten können drastische Folgen für die Zivilbevölkerung und das öffentliche Leben haben.[81] Aber auch in anderen Bereichen können sich durch Ransomware-Angriffe schwerwiegende Folgen ergeben. So standen in den Jahren 2022 und 2023 etwa Einrichtungen des Bildungswesens im Fokus krimineller Gruppen.[82] Durch Ransomware-Angriffe können – neben der Einschränkung der Verfügbarkeit von Ressourcen – vor allem finanzielle Schäden entstehen. Auch Privatpersonen können betroffen sein.

Ransomware-as-a-Service

„Der Anstieg der in den Umlauf gebrachten Ransomware-Dateien lässt sich auch darauf zurückführen, dass sie sich mittlerweile recht einfach herstellen lassen.“[83] Mit sogenannten Crimeware-Kits lassen sich Schadprogramme nach dem Baukastenprinzip zusammenstellen. Ransomware-Entwickelnde vermieten den Einsatz ihrer Schadsoftware an Cybercrimepartnerinnen bzw. -partner (Affiliates), die damit Ransomware-Angriffe durchführen und im Gegenzug Anteile des erpressten Lösegelds erhalten.[84] Ausgereifte technische Fertigkeiten sind hierbei deshalb nicht mehr zwingend

77 *BSI*, 2021, 5.
78 *BKA*, 2021, 44.
79 *Eckermann*, o. J.
80 *BKA*, 2019, 25.
81 *BKA*, 2021, 22.
82 *BKA*, 2023a, 26; 2024b, 3.
83 *Eckermann*, o. J.
84 *Eich*, 2023.

erforderlich. Diese Vorgehensweise führt zu einer starken Professionalisierung der Tatausübenden, die arbeitsteilig und international vernetzt agieren, was die Strafverfolgung erschwert.[85]

Modus Operandi „Double Extortion“

Eine besondere Variante der Ransomware-Angriffe ist die sogenannte *Double Extortion*. Bei dieser Methode verschlüsseln die Angreifenden nicht nur die Daten des Opfers, sondern entwenden diese auch vorab. Anschließend drohen sie damit, die gestohlenen Informationen zu veröffentlichen oder an Dritte zu verkaufen, sollte das Lösegeld nicht bezahlt werden. Diese Vorgehensweise erhöht den Druck auf die Opfer erheblich, da neben dem Verlust des Zugriffs auf wichtige Daten auch die Gefahr eines Datenlecks und der damit verbundenen reputations- und datenschutzrechtlichen Konsequenzen besteht. Die Drohung mit der Veröffentlichung sensibler Daten zwingt viele Opfer dazu, das Lösegeld zu zahlen, selbst wenn sie die Möglichkeit haben, ihre Daten aus Backups wiederherzustellen.[86] Double Extortion markiert somit eine Eskalation in der Schwere und den potenziellen Auswirkungen von Ransomware-Angriffen, da sie sowohl finanziellen als auch datenschutzrechtlichen Schaden anrichten kann.[87] Von dieser Art des kriminellen Vorgehens ist insbesondere das verarbeitende Gewerbe betroffen. Generell wird Ransomware gegen Unternehmen bzw. Einrichtungen jeder Größe und Branche eingesetzt.

So musste etwa die Landkreisverwaltung Anhalt-Bitterfeld des Landes Sachsen-Anhalt im Jahr 2021 nach eigenen Angaben fast zwei Wochen lang ihre Arbeit weitgehend einstellen, weil Kriminelle das Computersystem attackiert hatten. Zu dem Angriff bekannte sich die Tätergruppierung *Grief*.[88] Sie forderte ein Lösegeld in der Kryptowährung[89] Monero.[90] Ihrer Forderung verliehen die tatausübenden Personen durch die Veröffentlichung von 200 MB der entwendeten Daten auf einer Dedicated-Leak-Website im Darknet Nachdruck.[91] Eine Lösegeldzahlung wurde vom Landkreis verweigert.[92] Die Aufwendungen für den Landkreis, denkbar sind z. B. Kosten für die Reparatur seiner IT-Landschaft, beliefen sich insgesamt auf 2,5 Mio. Euro.[93]

---

85 *BKA*, 2021, 23.

86 Vgl. *BKA*, 2024a, 19.

87 *BSI*, 2023, 22 u. 38.

88 *Wieler*, 2021.

89 Kryptowährungen werden durch die Anwendung der Blockchain-Technologie geschaffen. Durch diese Technologie können Daten in dezentral verteilten Netzwerken manipulationssicher erhalten werden. Kryptowährungen werden nicht staatlich reguliert, dass bedeutet es gibt beispielsweise keine Einlagensicherung. Der Wert der Währung ergibt sich nur durch die Zahlungsbereitschaft der Anlegerinnen und Anleger – *BSI*, 2024a.

90 Die Verantwortlichen für Monero bezeichnen sie als „führende Kryptowährung mit einem Fokus auf private und zensurresistente Transaktionen“ – vgl. *Monero*, o. J.

91 *BKA*, 2022, 21.

92 *MDR*, 2024.

93 *Zeit Online*, 09.03.2024.

3.2 Diebstahl und Missbrauch von Identitätsdaten

Identitätsdiebstahl manifestiert sich als eine der vorherrschenden Bedrohungen im digitalen Raum. Dabei eignen sich die Cyberkriminellen persönliche Identitätsdaten unautorisiert an und missbrauchen sie für ihre Zwecke. Das Phänomen erstreckt sich über ein breites Spektrum illegaler Aktivitäten, angefangen bei Kreditkartenbetrug bis hin zu Szenarien des Identitätsmissbrauchs, die den Abschluss von Verträgen unter fremdem Namen beinhalten.[94]

Die Cyberkriminellen bedienen sich hier einer Reihe unterschiedlicher Techniken, um an die Daten zu gelangen. Die Praktik des Phishings etwa nutzt täuschend echte digitale Schnittstellen. Ziel ist es, das Opfer zur unbedarften Preisgabe sensibler Informationen zu verleiten, die für die Authentifizierung und Verifikation im Onlinehandel notwendig sind.[95]

Im Kontext von Malware zeigt sich eine ausgeklügelte Taktik der Cyberkriminellen: Sie entwickeln bösartige Softwares mit dem Ziel der Infiltration von Endgeräten, um dort Datensätze auszuspähen oder digitale Infrastrukturen zu kompromittieren. Insbesondere Trojanische Pferde zeigen diese Bedrohung, indem sie als gutartige Anwendungen auftreten, während sie simultan eine Konnektivität mit den Command-and-Control-Servern[96] der Angreifenden aufrechterhalten, um personenbezogene Daten zu extrahieren.[97]

Das Ausnutzen von Sicherheitslücken in Onlinediensten – englisch Exploitation – bietet Cyberkriminellen eine weitere Möglichkeit, Identitätsdaten zu entwenden. Die Angreifenden suchen gezielt nach Schwachstellen innerhalb der Softwarearchitektur, die ihnen unbefugten Zugriff gewähren, oft unter Verwendung von spezialisierten *Exploit-Kits*, die im Cyberraum verfügbar sind.[98]

Bei der Datenbankinfiltration nutzen die Angreifenden kompromittierte Zugangsdaten oder Schwachstellen aus, um massenhaft Identitätsdaten zu entwenden. Diese Verstöße haben nicht nur das Potenzial, Einzelne zu kompromittieren, sondern können auch die Integrität und das Vertrauen in die digitale Ökonomie verringern, indem sie die Daten einer Vielzahl von Nutzenden gefährden.[99]

Die verschiedenen Techniken wenden die Cyberkriminellen nicht isoliert, sondern häufig in Kombination an. Beispielsweise mag ein Phishing-Angriff den initialen Zugriffspunkt für die Verbreitung von Malware bereitstellen, die wiederum zur Ausnutzung von Sicherheitslücken oder zur Infiltration von Datenbanken eingesetzt werden kann.[100]

---

94 *BSI*, 2023, 17.

95 *BSI*, 2023, 17.

96 „Command-and-Control-Server (C&C-Server) sind eine Server-Infrastruktur, mit der Angreifer die in ein Botnetz integrierten infizierten Computersysteme (Bots) steuern. Bots (infizierte Systeme) melden sich in der Regel nach der Infektion bei dem C&C-Server des Angreifers [sic], um dessen Befehle entgegenzunehmen" – *BSI*, 2023, 89.

97 *BSI*, 2023, 13 u. 51.

98 *BSI*, 2016, 4.

99 *BSI*, 2023, 52.

100 *BSI*, 2023, 54.

3.3 Denial of Service-Angriffe

Distributed Denial of Service (DDoS)-Angriffe sind eine zunehmend präsente Gefahr in unserer digital vernetzten Gesellschaft. Diese Angriffe richten sich gegen die Verfügbarkeit und Integrität von Onlinediensten, indem sie mit einem Übermaß an Anfragen die zugrundeliegenden Systeme und Netzwerkinfrastrukturen überlasten. Durch das Sättigen der Bandbreite oder das Ausnutzen von Schwachstellen innerhalb spezifischer Anwendungen verhindern DDoS-Angriffe, dass legitime Zugriffe bearbeitet werden können.[101]

Die Methoden von DDoS-Angriffen sind vielseitig und komplex, angefangen bei großen Angriffen, die enorme Datenmengen generieren, bis hin zu Anwendungsebenen-Angriffen, die gezielt auf die Schwächen bestimmter Dienste abzielen. Der „Reflection-Angriff" ist ein weiteres Verfahren, das legitime Serveranfragen missbraucht, diese vervielfältigt und auf das Ziel umlenkt, um sowohl das Ziel als auch die dazwischenliegenden Netzwerke zu belasten.[102]

DDoS-Angriffe sind nicht nur eine technische Bedrohung, sondern haben auch einen direkten Einfluss auf die Gesellschaft. Sie untergraben das Vertrauen in Onlinedienste und können zu signifikanten wirtschaftlichen Schäden führen. Beispiele wie der Angriff auf den Internet-Infrastrukturdienstleister *Dyn* im Jahr 2016, der durch ein umfangreiches Botnetz aus IoT-Geräten (Internet of Things) zu umfassenden Dienstausfällen führte, zeigen, wie DDoS-Angriffe die Funktionsfähigkeit moderner Gesellschaften beeinträchtigen können.[103]

Ein weiteres Beispiel ist der Angriff auf *GitHub* im Jahr 2018, bei dem die Infrastruktur des Dienstes mit einer Rekordmenge an Datenverkehr geflutet wurde.[104] Diese Vorfälle verdeutlichen, wie DDoS-Angriffe Organisationen jeder Größe treffen können, von global agierenden Unternehmen bis hin zu lokalen Dienstleistern. Die Motivation hinter DDoS-Angriffen variiert von finanziellen Interessen, bei denen Angreifende Lösegeld fordern, bis hin zu politischen und persönlichen Motiven.[105] Die Verfügbarkeit von DDoS-as-a-Service-Diensten hat es zudem erleichtert, solche Angriffe auszuführen. Die Auswirkungen von DDoS-Angriffen sind nicht nur auf technische Störungen beschränkt; sie können erhebliche wirtschaftliche Verluste verursachen, Vertrauen erodieren und langfristigen Reputationsschaden anrichten. Diese Angriffe dienen oft als Ablenkung für andere bösartige Aktivitäten, wie das Eindringen in Netzwerke oder Datendiebstahl, was ihre Gefahren zusätzlich verstärkt.

„Im Zuge der international koordinierten ‚Operation Power Off' [sic] wurden unter Beteiligung des BKA im Dezember 2022 ca. 50 ‚DDoS-as-a-Service-Dienste' [sic] abgeschaltet."[106] Laut National Crime Agency wurden insgesamt 48 der beliebtesten Internetdomains beschlagnahmt, auf welchen DDoS-Booter-Dienste gezielt Webseiten und Server angegriffen haben. Die Operation habe zu sieben Verhaftungen von Administratoren geführt. Besonders betroffen seien – neben anderen Opfern – internationale KRITIS-Unternehmen gewesen.[107]

---

101 *BKA*, 2022, 23.
102 *BSI*, 2014, 1.
103 *Young*, 2022.
104 *Kottler*, 2018.
105 Siehe auch Kapitel 4.2.
106 *BKA*, 2023a, 3.
107 *NCA*, 2024.

3.4 Cybercrime as a Service

Cybercrime as a Service (CaaS) ermöglicht es Individuen und Organisationen weitgehend unabhängig von ihrem technischen Know-how, fortschrittliche Cyberangriffs-Tools und Dienstleistungen auf dem Schwarzmarkt zu erwerben oder zu mieten und somit erhebliche Bedrohungen im Cyberraum zu generieren.[108]

Die Struktur von CaaS ist inhärent modular und ermöglicht es Nutzenden, spezifische Komponenten oder vollständige Angriffskampagnen zu selektieren, die von DDoS-Angriffen bis zu komplexen Ransomware-Kampagnen reichen. Diese Dienstleistungen, häufig angeboten über das Darknet, beinhalten oft Anwendungssupport und regelmäßige Updates, was eine kontinuierliche Bedrohungslage schafft.[109] Im Kontext von Ransomware verdeutlicht das Konzept der Ransomware-as-a-Service (RaaS) die Verflechtung von CaaS mit spezifischen Cyberkriminalitätsphänomenen. RaaS erlaubt es auch technisch wenig versierten Akteurinnen bzw. Akteuren, Ransomware-Angriffe durchzuführen, indem sie Zugang zu vorgefertigten Ransomware-Kits erhalten, die gegen eine Provision der erpressten Gelder genutzt werden können.[110] Ähnlich verhält es sich mit dem Identitätsdiebstahl, wo CaaS-Marktplätze Tools und Daten für das Ausführen von Phishing-Angriffen oder den Erwerb gestohlener Identitätsdaten anbieten. Diese Aspekte unterstreichen die Rolle von CaaS als Katalysator für den Identitätsdiebstahl, indem sie den Erwerb und die Nutzung gestohlener Daten vereinfachen. Die Verbindung von CaaS zu DDoS-Angriffen manifestiert sich in der Bereitstellung von DDoS-for-hire-Diensten, welche umfangreiche Botnetze zur Durchführung von Angriffen zur Verfügung stellen. Diese Dienste senken die Schwelle für die Ausführung disruptiver DDoS-Kampagnen erheblich und erweitern das Spektrum der potenziellen Täterinnen oder Täter.[111]

Die Implikationen von CaaS sind weitreichend und stellen eine signifikante Herausforderung für die globale Cybersicherheit dar, da es die Eintrittsbarrieren für die Durchführung von Cyberangriffen drastisch senkt und gleichzeitig die Anonymität der Angreifenden wahrt. Die breite Verfügbarkeit dieser Dienste, auch in Kombination mit KI, erweitert das Potenzial für Cyberkriminalität über ein enges Spektrum technisch versierter Personen hinaus und eröffnet die Tür für eine Vielzahl von kriminellen Unternehmungen im Cyberraum.[112] Infolgedessen erfordert die Bekämpfung von CaaS eine verstärkte internationale Zusammenarbeit, die Entwicklung fortgeschrittener Sicherheitstechnologien und die Schaffung rechtlicher Rahmenbedingungen, die eine effektive Verfolgung dieser Form der organisierten Kriminalität ermöglichen.[113]

4 Erklärungsansätze

Zur Erklärung von Cyberkriminalität und zur Identifizierung von Handlungsmöglichkeiten können aus dem Spektrum kriminologischer Theorien der Routine Activity Approach und die Rational Choice Theory einen konzeptionellen Rahmen für die Analyse bieten.

---

[108] *BSI*, 2023, 89.
[109] *Luber*, 2023.
[110] *Luber*, 2023.
[111] *FBI*, o. J.
[112] *BKA*, 2024a, 24.
[113] *BSI*, 2023, 16 f.

4.1 Routine Activity Approach

Der Routine Activity Approach (RAA) von COHEN und FELSON aus dem Jahr 1979 kann auf das Phänomen Cybercrime i. e. S. angewendet werden. Der Ansatz basiert im Ursprung auf einer Untersuchung der steigenden Kriminalitätsrate in den USA in den 1960er Jahren.[114] Die Forschenden stellten in dieser Untersuchung fest, dass sich Tatgelegenheiten zumeist aus Routineaktivitäten ergaben. Die situationsbezogenen Einflussfaktoren kriminellen Verhaltens wurden von COHEN und FELSON in drei Bedingungen gefasst, die die Gefahr einer Viktimisierung bei einem simultanen Auftreten signifikant erhöhen. Zu Verwirklichung einer Straftet müssen demnach folgende Bedingungen vorliegen bzw. zusammentreffen:

1. eine motivierte Täterin bzw. ein motivierter Täter (motivated offender),
2. ein verfügbares und geeignetes Opfer oder Tatobjekt (availability of a suitable target) sowie
3. das Fehlen einer bzw. eines schutzbereiten Dritten (absence of capable guardian).[115]

Der RAA setzt sich nicht zum Ziel, die Motive der Täterinnen und Täter zu ergründen. Warum manche Personen tatgeneigt sind und sich über technische Sicherheitsmaßnahmen im Internet hinwegsetzen und andere keine Neigung verspüren, kann anhand des RAA folglich nicht erklärt werden. In Übereinstimmung mit den empirischen Erkenntnissen bzw. dem Modus Operandi der Phänomene und den Zielen der Straftaten (etwa der Überlastung von Systemen, Drohung mit der Veröffentlichung von Daten, Erpressung von „Lösegeldern“) können jedoch finanzielle und/oder politische Interessen für den Tatentschluss ausschlaggebend sein.

Insbesondere die Faktoren sozialer Wandel und Digitalisierung sind nach NEUBACHER für die Kriminalitätsentwicklung wesentlich.[116] Dadurch haben sich in den vergangenen Jahren zahlreiche Tatgelegenheiten und geeignete Ziele für die Seite der Cyberkriminellen ergeben. Ein geeignetes Ziel kann z. B. ein – hier digitales – Objekt mit ausreichendem Wert sein, das für die Täterin bzw. den Täter sichtbar und zugänglich ist.[117] Außerdem können neben dem Faktor Mensch die unsicheren IT-Systeme an sich ein geeignetes Einfallstor sein. Unzureichend gesicherte oder falsch konfigurierte Datenbanken, kritische Schwachstellen in Remote-Zugängen[118] oder fehlende Sicherheitsprogramme und Schutzmaßnahmen für gewerbliche oder private IT-Infrastrukturen ermöglichen es Angreifenden, in ein Zielsystem einzudringen und es zu kompromittieren. So besteht nach dem RAA besonders für kritische Infrastrukturen ein höheres Viktimisierungsrisiko, wenn die Unternehmen ihre Geschäftsmodelle in die digitale Welt verlagern, ohne dabei ausreichende technische Schutzmaßnahmen zu schaffen.

„Laut Risiko-Barometer 2021 der Allianz Global Corporate & Specialty gehören mangelnde Sicherheitsvorkehrungen und Data-Breaches[119] zu den größten Risiken für Unternehmen.“[120] Der Eintrittsvektor für Cyberangriffe ist nicht immer das Unternehmen selbst – oft nutzen die Kriminellen die Lieferkette des Unternehmens, die IT-Systeme der Geschäftspartnerin bzw. des

---

114 *Cohen/Felson* in: American Sociological Review, 1979, 588.

115 *Cohen/Felson* in: American Sociological Review, 1979, 589 f.

116 *Neubacher*, 2023, 72 ff. u. 114.

117 *Cohen/Felson* in: American Sociological Review, 1979, 595.

118 *Luber/Donner*, 2018.

119 Bei Data Breaches handelt es sich um eine Verletzung des Schutzes personenbezogener Daten. Sie können als Folge eines sicherheitsrelevanten Vorfalls in Unternehmen bzw. Organisationen zu einer Verletzung der Vertraulichkeit, Verfügbarkeit oder Integrität von personenbezogenen Daten führen. Dies kann sowohl die Mitarbeitenden als auch die Kundschaft oder anderweitige Geschäftskontakte betreffen – vgl. *Europäische Kommission*, o. J.

120 *BKA*, 2021 mit Verweis auf die *Allianz*, 2021.

Geschäftspartners oder des IT-Dienstleisters aus, um das eigentliche Ziel zu kompromittieren. Die Wertigkeit und das Schadenspotenzial von Cybercrimedelikten sind in den letzten Jahren stetig angestiegen. „Durch die Verzahnung von (digitalen) internationalen Lieferketten erhöht sich die Anzahl an potenziellen Eintrittsvektoren (...)."[121] Damit kann sich die Schadsoftware schnell über die komplette Lieferkette ausbreiten und somit „die Kompromittierung eines Teilsystems für einen kaskadenartigen Ausfall der gesamten Lieferkette sorgen."[122]

Viele Menschen nutz(t)en die Flexibilität des mobilen Arbeitens – nicht zuletzt während der COVID-19-Pandemie – und die Möglichkeiten digitaler Behördengänge.[123] Auch der weitere Ausbau von Dienstleistungen und Waren(-bestellungen) mit Hilfe des Internets steigert offenkundig die Anzahl der Tatgelegenheiten im Bereich Cybercrime, sofern keine Sicherungsmaßnahmen vorgenommen werden. Als Eintrittsvektor spielen nicht zuletzt auch Merkmale wie Profile von Benutzerinnen oder Benutzern und darauf veröffentlichte persönliche Informationen eine wichtige Rolle. Mit jedem erfolgreichen Angriff wird das kriminelle Potenzial der „*Underground Economy*" und damit ihre Möglichkeit, neue Malware zu entwickeln und komplexe Angriffe durchzuführen, erhöht.[124] „Erfolgreiche Angriffe auf diese ‚neue Flexibilität' haben zugleich starke Auswirkungen auf die Gesellschaft insgesamt", ggf. auch auf das subjektive Sicherheitsgefühl jedes einzelnen Menschen.[125]

4.2 Rational Choice Theory

Als ökonomischer Erklärungsansatz beschreibt die Rational Choice Theory (RCT) von BECKER das Verhalten von Menschen in Entscheidungssituationen.[126] Sie betrachtet den Menschen als „homo oeconomicus". Demnach wägen Menschen vor ihren Entscheidungen die jeweiligen Vor- und Nachteile ihres Handelns ab und entscheiden sich für die für sie günstigste Alternative. Folglich steigt für Menschen die Wahrscheinlichkeit, Straftaten zu begehen, sofern der Nutzen die Kosten überwiegt.[127] Als offensichtlicher Nutzen von Cybercrime kann der finanzielle Gewinn genannt werden. Extrinsisch motivierend kann Anerkennung oder Aufmerksamkeit der cyberkriminellen Community oder die mediale Berichterstattung sein. Intrinsisch motivierend kann etwa eine politische Überzeugung wirken.

Abzuwägen ist für die Seite der Cyberkriminellen vor allem das Entdeckungsrisiko durch die Strafverfolgungsbehörden.

> Allerdings ist die Ermittlung der Personen hinter den cyberkriminellen Aktivitäten „*langwierig und ressourcenintensiv. Gelingt die Ermittlung [von Tatverdächtigen], wird eine Festnahme oft dadurch erschwert, dass betreffende Personen sich in (...) einem safe haven*[128]*[,] wie [z. B.] Russland[,] aufhalten. Dies führt dazu, dass cyberkriminelle Handlungen aus dem Ausland rechtlich oft nicht geahndet und [Täterinnen und] Täter nicht an einer weiteren Tatausführung gehindert werden können.*
>
> *Eine sinnvolle Ergänzung personeller Ermittlungen ist insofern die bewusste Zerschlagung ... von kriminellen IT-Infrastrukturen[, welche die Kosten für Täterinnen und -täter erhöht.] Die bisherigen Erfolge der deutschen Polizeibehörden wie z. B. der Takedown der illegalen*

---

121 *Lorenz*, 2022.
122 *Lorenz*, 2022.
123 *BKA*, 2022, 36.
124 *BKA*, 2021, 38; 2022, 36 f.
125 *Lorenz*, 2022; *BKA*, 2022, 36.
126 *Becker*, 1982.
127 Vgl. weiterführend auch *Meier*, 2021, 38 ff.
128 Bei sogenannten safe haven handelt es sich um Staaten, in denen Täterinnen und Täter geduldet bzw. geschützt werden – *BKA*, 2024a, 25.

Verkaufsplattform Hydra Market, das Abschalten von DDoS-Booter-Diensten durch die Operation Power Off und die Zerschlagung der Emotet-Infrastruktur[129] *zeigen, dass eine Wiederinbetriebnahme vieler Infrastrukturen in der Regel kurzfristig nicht möglich und für die [Täterinnen und] Täter sehr ‚teuer' ist. (...)*

Ergänzt wird das technische Vorgehen gegen kriminelle Infrastrukturen durch den Zugriff auf illegale Gewinne der Tätergruppierungen [sic]. Ein Verfahren, das beide Elemente vereint, ist hierbei der erfolgreiche Zugriff auf die Serverinfrastruktur des Bitcoin-Mixers Chipmixer im März 2023. Neben der Zerschlagung der Infrastruktur gelang es, inkriminierte Bitcoins im Wert von ca. 90 Mio. Euro zu sichern und so dem kriminellen Wirtschaftskreislauf zu entziehen.

Der Infrastrukturansatz ermöglicht es [somit], kriminelle IT-Infrastrukturen zu zerschlagen und den Tätergruppierungen [sic] kriminelle Erträge zu entziehen. In Ergänzung zu personenbezogenen Ermittlungen können damit die Aktivitäten von [Cybertäterinnen und] Cybertätern für einen relevanten Zeitraum gestört und künftige Angriffe zumindest temporär eingeschränkt bzw. unterbunden werden. Zur umfassenden Bekämpfung von Cyberkriminalität zielt das BKA daher künftig verstärkt auf die Zerschlagung krimineller Infrastrukturen ab."[130]

5 Präventions - und Repressionsansätze

5.1 Cybersicherheitsstrategie der Bundesrepublik Deutschland von 2021

Die effektive Prävention und Repression von Cyberkriminalität erfordern eine Strategie, die technologische, soziale und politische Dimensionen umfasst. Die *Cybersicherheitsstrategie der Bundesrepublik Deutschland von 2021* betont die Notwendigkeit einer ganzheitlichen Herangehensweise. Diese Strategie integriert sich in die Bemühungen um die Stärkung der nationalen und internationalen Kooperation, die Förderung von Bildung und Aufklärung sowie die Entwicklung innovativer technologischer Lösungen.[131] Zur Realisierung der Ziele wurden bestehende Gesetze angepasst. So erhöht das *IT-Sicherheitsgesetz* Sicherheitsstandards für Betreiberinnen und Betreiber kritischer Infrastrukturen und stärkt die juristische Handhabe gegen Cyberdelikte.[132]

Ein weiteres Schlüsselelement der Strategie ist die Förderung der Resilienz gegenüber Cyberbedrohungen durch Bildungsinitiativen und die Sensibilisierung der Öffentlichkeit. Die Einbindung von Hackerclubs wie dem *Chaos Computer Club* und Fachtagungen spielen dabei eine wichtige Rolle, da sie den Austausch über Sicherheitslücken und deren Behebung fördern. Diese Foren bieten wertvolle Einblicke in aktuelle Bedrohungen und sind entscheidend für die Entwicklung gemeinschaftlicher Lösungsansätze. Unterstrichen wird zudem die Bedeutung der Zusammenarbeit zwischen staatlichen und nichtstaatlichen Organisationen, der Wirtschaft und der Zivilgesellschaft. Institutionen wie die polizeiliche Kriminalprävention der Länder und des Bundes (ProPK), die auf den Internetseiten „*polizei-beratung.de*" und „*polizeifuerdich.de*" Informationen bereitstellt, sind wichtig für die Aufklärung und Sensibilisierung in Bezug auf Cybersicherheit. Initiativen wie der *Safer-Internet-Day*[133] und der *Cyber Security Month*[134] tragen zur Förderung einer starken Sicherheitskultur bei.

---

129 *Europol*, 2021. Bei Emotet handelt es sich um den Namen einer Schadsoftware.
130 *BKA*, 2023a, 31.
131 *BMI*, 2021, 6 f.
132 *BSI*, o. J.b.
133 *Europäische Kommission*, 2024.
134 *ENISA*, o. J.

Die Strategie hebt auch die Notwendigkeit hervor, Risikogruppen durch zielgerichtete Präventionsmaßnahmen zu schützen. Herausforderungen ergeben sich für die Cybersicherheit etwa im Homeoffice, da Sicherheitslücken, die durch private Netzwerke und Endgeräte entstehen, sowie eine verminderte Kontrolle durch IT-Sicherheitsteams das Risiko erfolgreicher Cyberangriffe erhöhen. Die Zunahme von Angriffsvektoren aufgrund der dezentralen Arbeitsumgebungen erfordert innovative Sicherheitslösungen und eine stärkere Sensibilisierung der Mitarbeitenden für Cybersicherheitsrisiken.[135] Programme, die auf spezifische Gefahren im Internet hinweisen, werden von den Polizeibehörden bereitgestellt und sind hilfreich für die Sensibilisierung und den Schutz dieser Gruppen.

Die Cybersicherheitsstrategie ruft zu einer verstärkten Forschung und Entwicklung im Bereich der Cybersicherheit auf, um innovative Lösungsansätze zu entwickeln. Die Nutzung von KI und maschinellem Lernen für die frühzeitige Erkennung von Cyberangriffen und die Entwicklung automatisierter Schutzmechanismen ist hierbei von besonderer Bedeutung. Gleichzeitig wird die Rolle der Medienkompetenz als Schlüsselkompetenz in einer digitalisierten Welt hervorgehoben, die eine zentrale Säule der individuellen und kollektiven Cybersicherheitsstrategie bildet.[136] Kinder und Jugendliche, die in einer zunehmend digitalisierten Welt aufwachsen, und Senioren, die möglicherweise weniger mit den Risiken des Internets vertraut sind, sowie Unternehmen, insbesondere kleinere und mittlere Unternehmen (KMU), die oft nicht über die Ressourcen für umfassende Cybersicherheitsmaßnahmen verfügen, stellen zentrale Zielgruppen für präventive Maßnahmen dar.

5.2 Nationale und internationale Kooperation

Die Bedeutung der Prävention in Unternehmen wird durch die Arbeit von Behörden oder Organisationen wie dem *BSI* und *Verband der deutschen Internetwirtschaft (eco e. V.)* hervorgehoben, die die Implementierung von Sicherheitsmaßnahmen und die Schaffung von Standards für die Cybersicherheit vorantreiben. Die Zusammenarbeit von z. B. dem BSI und dem Verband der deutschen Internetwirtschaft (eco e. V.) mit Wirtschaftsunternehmen ist entscheidend für die Entwicklung und Implementierung von effektiven Sicherheitsstrategien.[137] Diese Partnerschaften ermöglichen es, spezialisiertes Wissen und Ressourcen zu bündeln, um so die Cyberresilienz von Unternehmen zu stärken. Darüber hinaus spielen branchenübergreifende Kooperationen eine Schlüsselrolle bei der Schaffung von Standards und Best Practices, die zum Schutz der gesamten digitalen Infrastruktur beitragen.

Auf institutioneller Ebene spielen das *BSI* und die *Zentralstelle für Informationstechnik im Sicherheitsbereich (ZITiS)*[138] tragende Rollen. Während das BSI für die Entwicklung von Sicherheitsstandards, die Überwachung der Cybersicherheitslage und die Bereitstellung von Empfehlungen zur IT-Sicherheit zuständig ist, unterstützt ZITiS die Sicherheitsbehörden mit technischen Lösungen zur Aufklärung und Prävention von Cyberkriminalität.

Darüber hinaus ist die *internationale Kooperation* angesichts der grenzüberschreitenden Natur von Cyberbedrohungen essenziell. Deutschland engagiert sich aktiv in multinationalen Foren, um globale Standards der Cybersicherheit zu fördern und die Verfolgung von Cyberkriminalität über Ländergrenzen hinweg zu verbessern. Bildungs- und Aufklärungsarbeit ergänzt die technischen und operativen Maßnahmen durch Kampagnen zur Sensibilisierung für Cyberrisiken und Weiterbildungsangebote im Bereich der IT-Sicherheit. Diese Maßnahmen zielen darauf ab, das Bewusstsein

[135] *BKA*, 2020b, 1 u. 17 ff.; *INFO GmbH Markt- und Meinungsforschung*, 2021, 16 f.
[136] *BMI*, 2021, 6 ff.
[137] *Eco e. V.*, o. J.
[138] *ZITiS*, o. J.

und die Kenntnisse der Bevölkerung zu erhöhen und individuelle sowie institutionelle Schutzmaßnahmen zu stärken.

5.3 Strafverfolgung

Im Bereich der *Strafverfolgung* gilt die Zerschlagung illegaler Infrastrukturen als ein effektiver Ansatz zur Bekämpfung von Cyberkriminalität ist. So konnten in den letzten Jahren unter Beteiligung des BKA folgende Ermittlungserfolge verbucht werden. Im Jahr 2023 unter anderem:

- Die Abschaltung der Plattform „Chipmixer", der größten Geldwäsche-Plattform im Darknet, und mehrerer krimineller Marktplätze wie zum Beispiel „Kingdom Market".[139]
- Zudem wurde mit „Quakbot" ein gefährliches Schadsoftware-Netzwerk zerschlagen. „Quakbot" kontrollierte über 700.000 infizierte Systeme im Internet, die für kriminelle Zwecke wie die Erpressung von Lösegeldzahlungen mittels Ransomware genutzt wurden.[140]

Im Jahr 2024 wurden unter anderem

- der weltweit agierende illegale Darknet-Marktplatz „Nemesis Market" mit über 150.000 Nutzenden und einem Warenangebot in den Bereichen Betäubungsmittel, betrügerisch erlangte Daten und Waren sowie verschiedenen Cybercrimeservices abgeschaltet.[141]
- Ebenso konnte der illegale Onlineservice „AegisTools.pw" unschädlich gestellt werden. Er ermöglichte die Verschleierung von Schadsoftware sowie den Diebstahl von Zugangsdaten.[142]
- Im Mai 2024 führte die „bislang größte internationale Cyber-Polizeioperation"[143] zum „Takedown", also der Beschlagnahme und Übernahme bzw. Stilllegung, von sechs der gefährlichsten Schadsoftware-Familien. Neben der Zerschlagung der Infrastruktur richtete sich die Operation „Endgame" auch gegen konkrete Akteure und ihre Finanzmittel.
- Im Zuge der Geldwäschebekämpfung gelang es im September 2024 insgesamt 47 in Deutschland gehostete Exchange Services der Underground Economy abzuschalten, die Tauschgeschäfte herkömmlicher Währungen und Kryptowährungen unter bewusst mangelhafter Umsetzung von gesetzlichen Vorgaben zur Geldwäschebekämpfung ermöglichten. „Das Angebot war darauf gerichtet, schnell, einfach und anonym Kryptowährungen in andere Krypto- oder digitale Währungen zu tauschen, um so deren Herkunft zu verschleiern."[144]
- Ende Oktober 2024 wurden im Rahmen einer international koordinierten Operation zwei Personen festgenommen, die beschuldigt werden, verschiedene kriminelle Infrastrukturen im Internet bereitgestellt und administriert zu haben, die unter anderem zum Handel mit Betäubungsmitteln in nicht geringer Menge sowie zur Computersabotage mittels sogenannter DDoS-Angriffe genutzt wurden.[145]

---

139 *BKA*, 2023b; *BMI*, 2024b.
140 *BMI*, 2024b.
141 *BKA*, 2024c.
142 *BKA*, 2024d.
143 *BKA*, 2024e.
144 *BKA*, 2024f.
145 *BKA*, 2024g.

- Bei der Festnahme eines Administrators der kriminellen Handelsplattform „Crimenetwork“ im Dezember 2024 wurden neben umfangreichen Beweismitteln und hochwertigen Fahrzeugen auch Vermögen im Wert von rund einer Million Euro in Kryptowerten sichergestellt. Die Plattform galt als größter deutschsprachiger Onlinemarktplatz für die Underground Economy und war seit vielen Jahren aktiv.[146]
- In der international abgestimmten Operation „Power Off“ im Dezember 2024 gingen insgesamt 15 Ländern gegen Cyberkriminalität vor. Im Mittelpunkt der von Europol koordinierten Aktion standen sogenannte Stresser-Dienste. Hierbei handelt es sich um bestimmte kriminelle Dienstleistungsplattformen im Internet, die das einfache und schnelle Durchführen von DDoS-Angriffen auch ohne tiefergehende technische Fähigkeiten ermöglichen. Es wurde weltweit sowohl gegen die IT-Infrastrukturen als auch gegen die an solchen Delikten beteiligten Personen vorgegangen. In diesem Zuge wurden insgesamt 27 Stresser-Dienste beschlagnahmt und vom Netz genommen. Die Daten wurden als Beweismittel gesichert und über 300 Nutzende identifiziert. Darüber hinaus erfolgten drei Festnahmen mutmaßlicher Administratoren in Deutschland und Frankreich.[147]

In diesem Jahr gelang den deutschen Strafverfolgungsbehörden im Rahmen der international abgestimmten Operation „Talent“ unter Führung der deutschen Behörden und Beteiligung von Europol vom 28. bis 30. Januar 2025 ein entscheidender Schlag gegen die beiden größten Handelsplattformen für Cybercrime im Internet.[148] Die Webseiten „nulled.to“ und „cracked.io“, die als Foren für Cybercrimedienstleistungen aufgebaut waren und damit wichtige Einstiegspunkte in die als „Underground Economy“ bezeichnete Schattenwirtschaft des Phänomenbereichs darstellten, konnten abgeschaltet, bei Durchsuchungsmaßnahmen zahlreiche Beschlagnahmen durchgeführt sowie zwei Personen festgenommen werden.

6 Fazit

Die Bedrohung durch Cybercrime i. e. S. hat sich zu einer der vordringlichsten Herausforderungen in der IT-Sicherheitslandschaft entwickelt. Der anhaltende Anstieg sowohl in qualitativer als auch quantitativer Hinsicht verdeutlicht die Notwendigkeit, die Ressourcen zu verstärken und einen Schwerpunkt auf die Bekämpfung von Cybercrimedelikten zu legen. Insbesondere die COVID-19-Pandemie hat die digitale Transformation beschleunigt und dadurch neue Angriffsflächen für Cyberkriminelle geschaffen. Der deutliche Anstieg von Phishing-Angriffen und die Zunahme von Ransomware-Attacken sowie Identitätsdiebstählen während der Pandemie zeigen, dass präventive Maßnahmen und die Sensibilisierung der Bevölkerung unabdingbar sind, um die digitale Sicherheit zu gewährleisten.

Die spezifischen Phänomene von Cybercrime wie Ransomware-Angriffe, der Missbrauch digitaler Identitätsdaten, DDoS-Angriffe und CaaS erfordern eine tiefgreifende Auseinandersetzung mit den technischen und sozialen Mechanismen, die diesen Delikten zugrunde liegen. Der Angriff auf den Landkreis Anhalt-Bitterfeld, bei dem Ransomware einen Katastrophenfall auslöste, sowie der DDoS-Angriff auf die Universität Duisburg-Essen zeigen exemplarisch nicht nur die unmittelbaren Auswirkungen auf die betroffenen Institutionen, sondern auch die potenziell weitreichenden Folgen[149] für die öffentliche Sicherheit sowie die ökonomischen und sozialen Folgen solcher Cyberangriffe.

---

146 *BKA*, 2024h.
147 *BKA*, 2024i.
148 *BKA*, 2025c.
149 Vgl. auch *BKA*, 2024a, 3 f.

Direkte finanzielle Verluste durch Betrug, Erpressung oder Diebstahl von geistigem Eigentum können öffentliche Institutionen und Unternehmen stark belasten. Darüber hinaus erfordern Angriffe oft kostspielige Investitionen in die Wiederherstellung der Systeme und können zu einem langfristigen Verlust des Kundenvertrauens führen. Sozial führt Cybercrime ggf. zu einer Verunsicherung in der Bevölkerung,[150] was die Akzeptanz und Nutzung digitaler Angebote beeinträchtigen kann. In diesem Sinne sollte Cybersicherheit nicht nur als technische, sondern als gesamtgesellschaftliche Aufgabe verstanden werden. Die Aspekte Bildung und Sensibilisierung sind in der Prävention von Cybercrime i. e. S. von erheblicher Bedeutung. Indem Bürgerinnen und Bürger, Unternehmen und Organisationen über die Risiken aufgeklärt und in den effektiven Schutz ihrer Daten und Systeme eingebunden werden, kann die Resilienz gegenüber Cyberangriffen erhöht werden.

Der russische Angriffskrieg auf die Ukraine hat die internationale Geopolitik und die Sicherheitslage im Cyberraum nachhaltig verändert. Die von der russischen Regierung medial vermittelten Drohungen gegen Unterstützerstaaten der Ukraine unterstreichen ein hohes Eskalationspotential für Cyberangriffe, auch auf kritische Infrastrukturen und öffentliche Einrichtungen. Dies verdeutlicht die Notwendigkeit einer international koordinierten Zusammenarbeit der Strafverfolgungsbehörden und einer proaktiven Gefahrenabwehr im Bereich Cybercrime. Die Reduzierung von Tatgelegenheiten und die Erhöhung des Entdeckungsrisikos sind hierbei wesentliche Faktoren in der Bekämpfung von Cyberkriminalität. Insbesondere die Rational Choice Theory betont, dass die Entscheidung zur Begehung von Delikten oft eine Abwägung von zu erwartendem Nutzen gegenüber den potenziellen Kosten und Risiken darstellt. Daraus folgt, dass die Erhöhung der Kosten und (Entdeckungs-)Risiken für potenzielle Cyberkriminelle durch effektive Sicherheitsmaßnahmen und eine konsequente Strafverfolgung von entscheidender Bedeutung sind.

Die Förderung von Forschung und Entwicklung im Bereich der Cybersicherheitstechnologien ist entscheidend, um innovative Lösungen zu entwickeln, die den fortgeschrittenen Methoden der Kriminellen einen Schritt voraus sind. Mit Blick auf die Zukunft könnte der Einsatz von KI durch Cyberkriminelle einen Wendepunkt in der Evolution von Cyberangriffen darstellen.[151] Insbesondere die Entwicklung und der Missbrauch von generativen KI-Modellen wie ChatGPT, beispielsweise für die automatisierte Erstellung von Phishing-Mails und Schadsoftware, senken die technischen Barrieren für kriminelle Aktivitäten erheblich.[152] Perspektivisch könnte KI die Effizienz und die Reichweite cyberkrimineller Aktivitäten erweitern und das Potenzial von KI als Eintrittsvektor für diverse Cyberangriffe verstärken. „KI-Modelle sind prinzipiell in der Lage, Schadsoftware zu programmieren, auf Fehler zu prüfen und ggf. auszubessern."[153] Die Reaktion auf diese Herausforderungen erfordert eine intensivierte Kooperation zwischen den IT-Sicherheitsunternehmen, der Privatwirtschaft und den Strafverfolgungsbehörden. Eine frühzeitige Einbindung der Polizeibehörden und eine schnelle, bundesweit koordinierte Reaktionsfähigkeit sind entscheidend, um Cyberangriffe effektiv abwehren zu können. Gleichzeitig bietet KI das Potenzial, die Bekämpfung von Cyberkriminalität

---

150 *Weber*, 2024, 38.

151 Vgl. *Europol* 2025, 21. Für den Bereich von Cybercrime i. w. S. stellen zudem sogenannte *Deepfakes,* durch KI erzeugte hyperrealistische Medieninhalte, eine neue Herausforderung dar, da sie zur Verbreitung von Desinformation oder zur Fälschung von Identitäten genutzt werden können. *„Lange Zeit war es sehr aufwändig, dynamische Medien, wie Videos oder Audiomitschnitte qualitativ hochwertig zu manipulieren. Durch Methoden aus dem Bereich der Künstlichen Intelligenz (KI) ist dies heute jedoch deutlich einfacher und Fälschungen können mit vergleichsweise wenig Aufwand und Expertise in einer hohen Qualität erstellt werden. Aufgrund der Nutzung von tiefen neuronalen Netzen (englisch: deep neural networks), werden solche Verfahren umgangssprachlich als ‚Deepfakes' bezeichnet" – BSI*, o. J.a.

152 *AISEC*, 2023.

153 *BKA*, 2024a, 14.

voranzutreiben, um Schwachstellen aufzudecken oder Softwareentwicklerinnen und Softwareentwicklern – beispielsweise durch Analyse automatisierter Code-Bestandteile – zu unterstützen.[154]

Es ist festzuhalten, dass der Kampf gegen Cybercrime i. e. S. eine der größten sicherheitspolitischen Herausforderungen unserer Zeit darstellt. Eine erfolgreiche Bekämpfung erfordert ein koordiniertes Vorgehen, das technische Sicherheitsmaßnahmen mit rechtlichen Rahmenbedingungen und der aktiven Einbindung der gesamten Gesellschaft zusammenführt.

Literaturverzeichnis

AISEC - Fraunhofer-Institut für Angewandte und Integrierte Sicherheit (2023): ChatGPT – neues Lieblingstool für Hacker? URL: cybersecurity.blog.aisec.fraunhofer.de/chatgpt-neues-lieblingstool-fuer-hacker/; letzter Zugriff am: 05.04.2024.

Allianz (2021): Allianz Risiko Barometer 2021: Covid-19-Trio an der Spitze der Unternehmensrisiken. München. URL: commercial.allianz.com/news-and-insights/news/allianz-risk-barometer-2021-de.html; letzter Zugriff am: 05.04.2024.

Becker, Gary S. (1982): Der ökonomische Ansatz zur Erklärung menschlichen Verhaltens. Tübingen: Mohr Siebeck.

Beisch, Natalie/*Schäfer*, Carmen (2020): Internetnutzung mit großer Dynamik: Medien, Kommunikation, Social Media. Ergebnisse der ARD/ZDF-Onlinestudie 2020. Korrigierte Fassung vom 1.11.2020. In: Media Perspektiven, Jg. 51, S. 462 – 481.

Birkel, Christoph/*Church*, Daniel/*Erdmann*, Anke/*Hager*, Alisa/*Leitgöb-Guzy*, Nathalie (2022): Sicherheit und Kriminalität in Deutschland - SKiD 2020. Bundesweite Kernbefunde des Viktimisierungssurvey des Bundeskriminalamts und der Polizei der Länder. Stand: August 2020 Auflage. Wiesbaden: Bundeskriminalamt.

Bitkom e. V. (2021): Wirtschaftsschutz 2021. Berlin. URL: bitkom.org/Presse/Presseinformation/Angriffsziel-deutsche-Wirtschaft-mehr-als-220-Milliarden-Euro-Schaden-pro-Jahr.

Bitkom e. V. (2022): Wirtschaftsschutz 2022. Berlin. URL: bitkom.org/sites/main/files/2022-08/Bitkom-Charts_Wirtschaftsschutz_Cybercrime_31.08.2022.pdf; letzter Zugriff am: 15.03.2024.

Bitkom e. V. (2023): Wirtschaftsschutz 2023. Berlin. URL: bitkom.org/sites/main/files/2023-09/Bitkom-Charts-Wirtschaftsschutz-Cybercrime.pdf; letzter Zugriff am: 15.03.2024.

Bitkom e. V. (2024): Wirtschaftsschutz 2024. Berlin. URL: bitkom.org/Presse/Presseinformation/Wirtschaftsschutz-2024; letzter Zugriff am: 28.08.2024.

BKA - Bundeskriminalamt (o. J.): Cybercrime. Was ist Cybercrime? URL: bka.de/DE/UnsereAufgaben/Deliktsbereiche/Cybercrime/cybercrime_node.html; letzter Zugriff am: 05.04.2024.

BKA - Bundeskriminalamt (2017): Cybercrime. Bundeslagebild 2016. Wiesbaden. URL: bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2016.pdf?__blob=publicationFile&v=2; letzter Zugriff am: 08.04.2024.

[154] *AISEC*, 2023.

BKA - Bundeskriminalamt (2019): Cybercrime. Bundeslagebild 2018. URL: bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2018.pdf?__blob=publicationFile&v=4; letzter Zugriff am: 12.04.2024.

BKA - Bundeskriminalamt (2020a): Cybercrime. Bundeslagebild 2019. URL: bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2019.pdf?__blob=publicationFile&v=3; letzter Zugriff am: 27.04.2024.

BKA - Bundeskriminalamt (2020b): Sonderauswertung Cybercrime in Zeiten der Corona-Pandemie. URL: bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeSonderauswertungCorona2019.pdf?__blob=publicationFile&v=3.

BKA - Bundeskriminalamt (2021): Cybercrime. Bundeslagebild 2020. Wiesbaden. URL: bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2020.html?nn=28110; letzter Zugriff am: 14.03.2024.

BKA - Bundeskriminalamt (2022): Cybercrime. Bundeslagebild 2021. Wiesbaden. URL: bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2021.html?nn=28110; letzter Zugriff am: 14.03.2024.

BKA - Bundeskriminalamt (2023a): Cybercrime. Bundeslagebild 2022. Wiesbaden. URL: bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2022.pdf?__blob=publicationFile&v=5; letzter Zugriff am: 14.03.2024.

BKA - Bundeskriminalamt (2023b): BKA schaltet weltweit größten Geldwäschedienst im Darknet ab. Server der Plattform „ChipMixer“ beschlagnahmt und Rekordsumme von rund 44 Millionen Euro in Bitcoin sichergestellt. Wiesbaden. URL: https://bka.de/DE/Presse/Listenseite_Pressemitteilungen/2023/Presse2023/230314_Geldwaesche_Darknet.html; letzter Zugriff am: 28.02.2025.

BKA - Bundeskriminalamt (2024a): Cybercrime. Bundeslagebild 2023. Wiesbaden. URL: bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2023.html?nn=28110; letzter Zugriff am: 09.09.2024.

BKA - Bundeskriminalamt (2024b): Aufgliederung der Straftaten nach Schadenshöhe - nur für Delikte mit Schadenserfassung. Tabelle 07. V1.0. URL: bka.de/SharedDocs/Downloads/DE/Publikationen/PolizeilicheKriminalstatistik/2023/Bund/Faelle/BU-F-07-T07-Schaden_xls.xlsx?__blob=publicationFile&v=3; letzter Zugriff am: 12.04.2024.

BKA - Bundeskriminalamt (2024c): Illegaler Darknet-Marktplatz „Nemesis Market“ abgeschaltet. Plattform mit über 150.000 Nutzenden ermöglichte massenhaften Handel mit Betäubungsmitteln, betrügerisch erlangten Daten sowie verschiedenen Cybercrime-Services. Pressemitteilung der Generalstaatsanwaltschaft Frankfurt am Main -ZIT- und des Bundeskriminalamtes. Wiesbaden. URL: https://bka.de/DE/Presse/Listenseite_Pressemitteilungen/2024/Presse2024/240321_PM_Nemesis_Market.html; letzter Zugriff am: 28.02.2025.

BKA - Bundeskriminalamt (2024d): Illegaler Online-Service „AegisTools.pw“ abgeschaltet. Mutmaßlicher Betreiber identifiziert - Plattform ermöglichte Verschleierung von Schadsoftware sowie Diebstahl von Zugangsdaten. Pressemitteilung der Generalstaatsanwaltschaft Koblenz und des Bundeskriminalamtes. Wiesbaden. URL: https://bka.de/DE/Presse/Listenseite_Pressemitteilungen/2024/Presse2024/240410_PM_Abschaltung_illegaler_Onlineservice.html; letzter Zugriff am: 28.02.2025.

BKA - Bundeskriminalamt (2024e): Bundeskriminalamt und internationalen Partnern gelingt bisher größter Schlag gegen weltweite Cybercrime. Zehn internationale Haftbefehle und vier vorläufige Festnahmen ++ Deutschland initiiert und koordiniert „Takedowns“ der gefährlichsten Schadsoftware-Familien. Gemeinsame Pressemitteilung der Generalstaatanwaltschaft Frankfurt am Main - ZIT- und des Bundeskriminalamtes. Wiesbaden. URL: https://bka.de/DE/Presse/Listenseite_Pressemitteilungen/2024/Presse2024/240530_PM_Endgame.html; letzter Zugriff am: 28.02.2025.

BKA - Bundeskriminalamt (2024f): Cybercrime: Erfolgreicher Schlag gegen die Infrastruktur von digitalen Geldwäschern der Underground Economy. BKA und ZIT schalten 47 in Deutschland gehostete Exchange-Services ab. Wiesbaden. URL: https://bka.de/DE/Presse/Listenseite_Pressemitteilungen/2024/Presse2024/240919_PM_finalexchange.html; letzter Zugriff am: 28.02.2025.

BKA - Bundeskriminalamt (2024g): Festnahmen von mutmaßlichen Cybercrime-Straftätern. Erneuter Schlag gegen Underground Economy im Internet. Wiesbaden. URL: https://bka.de/SharedDocs/Kurzmeldungen/DE/Kurzmeldungen/241031_Festnahme_Cybercrime.html; letzter Zugriff am: 28.02.2025.

BKA - Bundeskriminalamt (2024h): Administrator des Online-Marktplatzes „Crimenetwork“ festgenommen. URL: https://bka.de/SharedDocs/Kurzmeldungen/DE/Kurzmeldungen/241203_Festnahme_Crimenetwork.html; letzter Zugriff am: 28.02.2025.

BKA - Bundeskriminalamt (2024i): Operation „Power OFF“: weltweiter Schlag gegen Cybercrime-Infrastruktur. URL: https://bka.de/SharedDocs/Kurzmeldungen/DE/Kurzmeldungen/241211_Operation_PowerOFF_2024.html; letzter Zugriff am: 28.02.2025.

BKA - Bundeskriminalamt (2025a): Aufgliederung der Straftaten nach Schadenshöhe - nur für Delikte mit Schadenserfassung. Tabelle 07. V1.0. URL: bka.de/SharedDocs/Downloads/DE/Publikationen/PolizeilicheKriminalstatistik/2024/Bund/Faelle/BU-F-07-T07-Schaden_xls.xlsx?__blob=publicationFile&v=2; letzter Zugriff am: 08.04.2025.

BKA - Bundeskriminalamt (2025b): Aufgliederung der Straftaten nach Schadenshöhe. Tabelle 07-A. V1.0. URL: bka.de/SharedDocs/Downloads/DE/Publikationen/PolizeilicheKriminalstatistik/2024/Bund/Ausland/Faelle/BU-F-13a-T06-A-Faelle-Tatortstaat-Ausland_xlsx.xlsx?__blob=publicationFile&v=5; letzter Zugriff am: 10.04.2025.

BKA - Bundeskriminalamt (2025c): Strafverfolgungsbehörden schalten die zwei weltweit größten Cybercrime-Foren mit rund zehn Millionen registrierten Nutzern ab. URL: https://bka.de/SharedDocs/Kurzmeldungen/DE/Kurzmeldungen/250130_Operation_Talent.html; letzter Zugriff am: 28.02.2025.

BMI - Bundesministerium des Innern, für Bau und Heimat (2021): Cybersicherheitsstrategie für Deutschland 2021. Berlin. URL: bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2021/09/cybersicherheitsstrategie-2021.pdf?__blob=publicationFile&v=2; letzter Zugriff am: 05.04.2024.

BMI - Bundesministerium des Innern und für Heimat (2024a): Polizeiliche Kriminalstatistik 2023. Ausgewählte Zahlen im Überblick. Heft V1.0. Berlin. URL: bka.de/SharedDocs/Downloads/DE/Publikationen/PolizeilicheKriminalstatistik/2023/FachlicheBroschueren/IMK-Bericht.pdf?__blob=publicationFile&v=6; letzter Zugriff am: 09.04.2024.

BMI - Bundesministerium des Innern und für Heimat (2024b): Cyberkriminalität erneut gestiegen: Sicherheitsbehörden zerschlagen kriminelle Infrastrukturen. Bundesinnenministerin Faeser, BKA-

Präsident Münch und BSI-Präsidentin Plattner haben Bundeslagebild für 2023 vorgestellt. Berlin. URL: https://bmi.bund.de/SharedDocs/pressemitteilungen/DE/2024/05/bka-lagebild-cyberkriminalitaet.html; letzter Zugriff am: 28.02.2024.

BMI - Bundesministerium des Innern und für Heimat (2025): Polizeiliche Kriminalstatistik 2024. Ausgewählte Zahlen im Überblick. Heft V2.0. Berlin. URL: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/PolizeilicheKriminalstatistik/2024/FachlicheBroschueren/IMK-Bericht.pdf?__blob=publicationFile&v=7; letzter Zugriff am: 08.04.2025.

BMI/BMJV - Bundesministerium des Innern und für Heimat/Bundesministerium der Justiz und für Verbraucherschutz (2021): Dritter Periodischer Sicherheitsbericht. URL: bmj.de/DE/Service/Fachpublikationen/Dritter_Periodischer_Sicherheitsbericht.html; letzter Zugriff am: 12.04.2023.

BSI - Bundesamt für Sicherheit in der Informationstechnik (o. J.a): Deepfakes - Gefahren und Gegenmaßnahmen. URL: bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Kuenstliche-Intelligenz/Deepfakes/deepfakes_node.html; letzter Zugriff am: 05.04.2024.

BSI - Bundesamt für Sicherheit in der Informationstechnik (o. J.b): Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0). Neues IT-Sicherheitsgesetz für eine moderne Cybersicherheit. URL: bsi.bund.de/DE/Das-BSI/Auftrag/Gesetze-und-Verordnungen/IT-SiG/2-0/it_sig-2-0_node.html; letzter Zugriff am: 05.04.2024.

BSI - Bundesamt für Sicherheit in der Informationstechnik (2014): Maßnahmen gegen Reflection Angriffe: Heft BSI-CS 096. Bonn. URL: allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_096.pdf?__blob=publicationFile&v=1#:~:text=Die%20Verwendung%20von%20SNMPv3%20bietet,und%20Funk%20tionen%20eingeschr%C3%A4nkt%20werden.; letzter Zugriff am: 05.04.2024.

BSI - Bundesamt für Sicherheit in der Informationstechnik (2016): Lagedossier Ransomware. Stand Mai 2016. Bonn. URL: bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Lagedossier_Ransomware.pdf?__blob=publicationFile&v=2; letzter Zugriff am: 05.04.2024.

BSI - Bundesamt für Sicherheit in der Informationstechnik (2021): Ransomware. Bedrohungslage, Prävention & Reaktion 2021. URL: bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Ransomware.pdf?__blob=publicationFile&v=2.

BSI - Bundesamt für Sicherheit in der Informationstechnik (2023): Die Lage der IT-Sicherheit in Deutschland 2023. URL: bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2023.html?nn=129410.

BSI - Bundesamt für Sicherheit in der Informationstechnik (2024a): Blockchain macht Daten praktisch unveränderbar. Kryptowährung als prominentester Anwendungsfall einer Blockchain-Technologie. URL: bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Technologien_sicher_gestalten/Blockchain-Kryptowaehrung/blockchain-kryptowaehrung_node.html; letzter Zugriff am: 01.10.2024.

BSI - Bundesamt für Sicherheit in der Informationstechnik (2024b): Malware. URL: bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Gefaehrdungen/Malware/malware_node.html#:~:text=Malware%20ist%20ein%20Kunstwort%2C%20das,Regel%20ohne%20Wissen%20des%20Benutzers.; letzter Zugriff am: 01.10.2024.

Bundeswehr (o. J.): Zentrum für Cyber-Sicherheit der Bundeswehr. Gebündelte Cyber-Defence Fähigkeiten der Bundeswehr. URL: bundeswehr.de/de/organisation/cyber-und-informationsraum/kommando-und-organisation-cir/kommando-cyber-und-informationsraum/zentrum-fuer-cyber-sicherheit-der-bundeswehr; letzter Zugriff am: 05.04.2024.

Chainalysis (2024): The 2024 Crypto Crime Report. The latest trends in ransomware, scamsm hacking and more. URL: go.chainalysis.com/crypto-crime-2024.html; letzter Zugriff am: 29.04.2024.

Cohen, Lawrence E./*Felson*, Marcus (1979): Social Change and Crime Rate Trends: A Routine Activity Approach. In: American Sociological Review, Jg. 44, S. 588 – 608.

Coveware (2024): New Ransomware Reporting Requirements Kick in as Victims Increasingly Avoid Paying. URL: coveware.com/blog/2024/1/25/new-ransomware-reporting-requirements-kick-in-as-victims-increasingly-avoid-paying; letzter Zugriff am: 05.04.2024.

Dreißigacker, Arne/*Skarczinski*, Bennet von/*Wollinger*, Gina R. (2021): Cyberangriffe gegen Unternehmen in Deutschland. Ergebnisse einer Folgebefragung 2020. Forschungsberichte: Heft Nr. 162. Hannover. URL: kfn.de/wp-content/uploads/Forschungsberichte/FB_162.pdf; letzter Zugriff am: 05.04.2024.

Eckermann, Ines M. (o. J.): Was ist eigentlich Ransomware? URL: gdata.de/ratgeber/was-ist-eigentlich-ransomware; letzter Zugriff am: 05.04.2024.

eco e. V. - Verband der Internetwirtschaft (o. J.): Verbandspartner. URL: eco.de/ueber-eco/eco-partner/; letzter Zugriff am: 05.04.2024.

Eich, Jakob (2023): Unternehmen lassen sich weniger erpressen. URL: dertreasurer.de/news/risikomanagement/unternehmen-lassen-sich-weniger-erpressen-35993/; letzter Zugriff am: 10.04.2024.

ENISA - European Union Agency for Cybersecurity (o. J.): European Cybersecurity Month. URL: enisa.europa.eu/topics/cybersecurity-education/awareness-campaigns/european-cyber-security-month; letzter Zugriff am: 05.04.2024.

Europäische Kommission (o. J.): Was ist eine Verletzung des Schutzes personenbezogener Daten und was ist in einem solchen Fall zu tun? URL: commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-data-breach-and-what-do-we-have-do-case-data-breach_de; letzter Zugriff am: 10.04.2024.

Europäische Kommission (2024): Safer Internet Day. URL: digital-strategy.ec.europa.eu/en/policies/safer-internet-day; letzter Zugriff am: 05.04.2024.

Europol - Europäisches Polizeiamt (2021): World's most dangerous malware EMOTET disrupted through global action. URL: europol.europa.eu/media-press/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action; letzter Zugriff am: 05.04.2024.

Europol - Europäisches Polizeiamt (2022): European Multidisciplinary Platform Against Criminal Threats (EMPACT). URL: europol.europa.eu/crime-areas-and-statistics/empact; letzter Zugriff am: 27.04.2024.

Europol - Europäisches Polizeiamt (2024): European Cybercrime Centre - EC3. Combating crime in a digital age. URL: europol.europa.eu/about-europol/european-cybercrime-centre-ec3; letzter Zugriff am: 05.04.2024.

Europol - Europäisches Polizeiamt (2025): The changing DNA of serious and organised crime. EU Serious and Organised Crime Threat Assessment 2025 (EU-SOCTA). URL: europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf; letzter Zugriff am: 24.03.2025.

FBI - Federal Bureau of Investigation (o. J.): The FBI and International Law Enforcement Partners Intensify Efforts to Combat Illegal DDoS Attacks. URL: fbi.gov/contact-us/field-offices/anchorage/fbi-intensify-efforts-to-combat-illegal-ddos-attacks; letzter Zugriff am: 05.04.2024.

GAO - United States Government Accountability Office (2017): Costs of Crime. Experts Report Challenges Estimating Costs and Suggest Improvements to Better Inform Policy Decisions. Report to Congressional Requesters: Heft GAO-17-732. URL: gao.gov/assets/gao-17-732.pdf; letzter Zugriff am: 08.04.2024.

Greenfield, Victoria A./*Paoli*, Letizia (2013): A framework to assess the harms of crimes. In: The British Journal of Criminology, Jg. 53, S. 864 – 885.

Hillebrand, Annette/*Niederprüm*, Antonia/*Schäfer*, Saskja/*Thiele*, Sonja/*Henseler-Unger*, Iris (2017): Aktuelle Lage der IT-Sicherheit in KMU. Bad Honnef. URL: wik.org/fileadmin/files/_migrated/news_files/WIK-Studie_Aktuelle_Lage_der_IT-Sicherheit_in_KMU_Langfassung__2_.pdf; letzter Zugriff am: 29.04.2024.

Huber, Edith (2019): Cybercrime. Eine Einführung. Wiesbaden: Springer. URL: dokumen.pub/download/cybercrime-eine-einfhrung-3658261498-9783658261498-9783658261504.html; letzter Zugriff am: 15.03.2024.

INFO GmbH Markt- und Meinungsforschung (2021): IT-Sicherheit im Home-Office. Bundesamt für Sicherheit in der Informationstechnik (BSI) veröffentlicht Studie IT-Sicherheit im Home-Office im Jahr 2020 unter Pandemie-Berücksichtigung. URL: infogmbh.de/it-sicherheit-im-home-office/; letzter Zugriff am: 08.04.2024.

Interpol - Internationale kriminalpolizeiliche Organisation (o. J.): Cybercrime – #YouMayBeNext. URL: interpol.int/Crimes/Cybercrime/Cybercrime-YouMayBeNext; letzter Zugriff am: 08.04.2024.

Kottler, Sam (2018): February 28th DDoS Incident Report. URL: github.blog/2018-03-01-ddos-incident-report/; letzter Zugriff am: 05.04.2024.

Lorenz, Wolf-Dietrich (2022): Quo vadis, Cybercrime? URL: krankenhaus-it.de/item.1538/quo-vadis-cybercrime.html; letzter Zugriff am: 24.03.2025.

Luber, Stefan (2023): Was ist Cybercrime-as-a-Service (CaaS)? URL: security-insider.de/was-ist-cybercrime-as-a-227da54abd15f73a0f3072b4e798b1ed/; letzter Zugriff am: 08.04.2024.

Luber, Stefan/*Donner*, Andreas (2018): Was ist Remote Access? URL: ip-insider.de/was-ist-remote-access-a-606391/; letzter Zugriff am: 08.04.2024.

MDR - Mitteldeutscher Rundfunk (2024): Neue Zahlen: Cyberangriff kostet ANhalt-Bitterfeld 2,5 Millionen Euro. URL: mdr.de/nachrichten/sachsen-anhalt/dessau/anhalt/cyberangriff-kreis-kosten-teurer-als-gedacht-102.html; letzter Zugriff am: 02.10.2024.

Meier, Bernd-Dieter (2021): Kriminologie. 6. Auflage. München: C. H. Beck.

Monero (o. J.): Was ist Monero (XMR)? URL: getmonero.org/de/get-started/what-is-monero/; letzter Zugriff am: 08.04.2024.

Münch, Holger (2020): Grußwort. In: wehr technik Spezial, Jg. 52, S. 6 – 7.

NCA - National Crime Agency (2024): NCA infiltrates world's most profilic DDoS-for-hire service. Cyber crime. URL: nationalcrimeagency.gov.uk/news/nca-infiltrates-world-s-most-prolific-ddos-for-hire-service; letzter Zugriff am: 10.09.2024.

Neubacher, Frank (2023): Kriminologie. 5 Auflage. Baden-Baden: Nomos.

Paoli, Letizia u. a. (2018): Belgian Cost of Cybercrime: Measuring cost and impact of cybercrime in Belgium. Final Report. Brüssel. URL: belspo.be/belspo/brain-be/projects/FinalReports/BCC_Final%20Report.pdf; letzter Zugriff am: 08.04.2024.

Recorded Future (2023): Russia's War Against Ukraine Disrupts the Cybercriminal Ecosystem: Heft CTA-RU-2023-0223. URL: go.recordedfuture.com/hubfs/reports/cta-2023-0223.pdf; letzter Zugriff am: 08.04.2024.

Riesner, Lars/*Glaubitz*, Christoffer (2020): Sicherheit und Kriminalität in Schleswig-Holstein. Kernbefunde des Viktimisierungssurvey 2019.

Rüdiger, Thomas-Gabriel/*Bayerl*, Petra S. (2020): Cyberkriminologie. In: Rüdiger, Thomas-Gabriel/Bayerl, Petra Saskia (Hg.). Cyberkriminologie. Kriminologie für das digitale Zeitalter. Wiesbaden: Springer. 2020. S. 3 – 12.

SoSafe (2024): Cybercrime-Trends 2024. Die größten Angriffstrends und Best Practices für mehr Sicherheit. Köln. URL: sosafe-awareness.com/de/ressourcen/reports/cybercrime-trends/; letzter Zugriff am: 08.04.2024.

The White House (2023): International Counter Ransomware Initiative 2023 Joint Statement. URL: whitehouse.gov/briefing-room/statements-releases/2023/11/01/international-counter-ransomware-initiative-2023-joint-statement/; letzter Zugriff am: 27.04.2024.

Verbraucherzentrale e. V. (2023): Welche Folgen Identitätsdiebstahl im Internet haben kann. URL: verbraucherzentrale.de/wissen/digitale-welt/datenschutz/welche-folgen-identitaetsdiebstahl-im-internet-haben-kann-17750; letzter Zugriff am: 08.04.2024.

Veritas (2023): Datenrisiko-Management. Die Marktlage - von Cyber zu Compliance. Dach-Bericht 2023. München.

Weber, Christine (2024): Kosten und Schäden durch Cyber-Kriminalität in Deutschland. Aktuelles aus der kriminalistisch-kriminologischen Forschung. Referat IZ 36 - Cybercrimeforschung. Forschungsberichte: Heft 1/2024. URL: bka.de/SharedDocs/Downloads/DE/Publikationen/Publikationsreihen/Forschungsergebnisse/2024KKAktuell_Kosten_Schaeden_Cyberkriminalitaet.pdf?__blob=publicationFile&v=4; letzter Zugriff am: 08.04.2024.

Wieler, Herbert (2021): DoppelPaymer-Ransomware erhält rebrand zur Grief-Ransomware. URL: infopoint-security.de/doppelpaymer-ransomware-erhaelt-rebrand-zur-grief-ransomware%20/a28342/; letzter Zugriff am: 08.04.2024.

Young, Kelli (2022): Cyber Case Study: The Mirai DDoS Attack on Dyn. URL: coverlink.com/case-study/mirai-ddos-attack-on-dyn/; letzter Zugriff am: 05.04.2024.

Zeit Online (2024): Cyberangriff kostete Anhalt-Bitterfeld 2,5 Millionen Euro. Kommunen. URL: zeit.de/news/2024-03/09/cyberangriff-kostete-anhalt-bitterfeld-2-5-millionen-euro; letzter Zugriff am: 09.03.2024.

ZITiS - Zentrale Stelle für Informationstechnik im Sicherheitsbereich (o. J.): Wer wir sind. URL: zitis.bund.de/DE/WerWirSind/werwirsind_node.html; letzter Zugriff am: 08.04.2024.

Impressum

Herausgeber
Bundeskriminalamt, 65173 Wiesbaden
Internet: **www.bka.de**

Stand
April 2025

Gestaltung
Bundeskriminalamt – Kriminalistisches Institut, 65173 Wiesbaden

Weitere Publikationen des Bundeskriminalamts zum Herunterladen und zum Bestellen finden Sie unter:
www.bka.de

Diese Publikation wird vom Bundeskriminalamt im Rahmen seiner Öffentlichkeitsarbeit herausgegeben. Die Publikation wird kostenlos abgegeben und ist nicht zum Verkauf bestimmt. Nachdruck und sonstige Vervielfältigung, auch auszugsweise, nur mit Quellenangabe des Bundeskriminalamtes.