Bundeslagebild Cybercrime

Deutschland 2025

Bundeskriminalamt

BKA

Allgemeine Informationen

Das Bundeslagebild Cybercrime wird durch das Bundeskriminalamt (BKA) in Erfüllung seiner Zentralstellenfunktion erstellt. Es enthält die aktuellen Erkenntnisse und Entwicklungen im Bereich der Cyberkriminalität in Deutschland und bildet insbesondere die diesbezüglichen Ergebnisse polizeilicher Strafverfolgungstätigkeiten ab.

Schwerpunkt des Bundeslagebildes Cybercrime sind die Delikte, die sich gegen das Internet und informationstechnische Systeme richten – sogenannte Cybercrime im engeren Sinne (CCieS).

Eine Grundlage für den statistischen Teil des Lagebildes sind die Daten der Polizeilichen Kriminalstatistik (PKS). Da bei einem Großteil der Straftaten der CCieS Schäden in Deutschland verursacht werden, der Aufenthaltsort der Tatverdächtigen aber unbekannt ist oder der Angriff aus dem Ausland heraus ausgeführt wird, bedarf es zur ganzheitlicheren Beschreibung des Phänomens neben der Darstellung der Inlandstaten (Inlands-PKS) auch einer Betrachtung der Auslandstaten (Auslands-PKS).[1] Im Folgenden wird für diese Fälle weiter der Begriff „Auslandstat“ verwendet, auch wenn im Bereich Cybercrime bei einem weit überwiegenden Teil der Fälle der Handlungsort der Tatverdächtigen unbekannt ist.

Sowohl in der Inlands- als auch in der Auslands-PKS wird das sogenannte Hellfeld abgebildet, also die polizeilich bekannt gewordene Kriminalität. Valide Aussagen und Einschätzungen zu Art und Umfang des komplementären Dunkelfeldes, also den Straftaten, die der Polizei nicht bekannt sind, können aus den statistischen Grunddaten der PKS alleine nicht abgeleitet werden. Im Bereich der Cyberkriminalität ist das Dunkelfeld Studien zufolge weit überdurchschnittlich ausgeprägt, sodass es für eine quantitativ und qualitativ zutreffende Lagebeschreibung von besonderer Bedeutung ist, polizeiexterne Informationen einzubeziehen. Zu diesem Zweck fließen in das Bundeslagebild Cybercrime auch Erkenntnisse und Einschätzungen anderer Behörden sowie ausgewählter privatwirtschaftlicher oder wissenschaftlicher Organisationen ein.

Herausgehobene Sachverhalte und Beispiele operativer Maßnahmen wurden teilweise von Länderdienststellen zugeliefert. Diese sind im Text als Quellverweise entsprechend ausgewiesen.

An verschiedenen Stellen des Bundeslagebilds Cybercrime 2025 sind QR-Codes eingebettet, über die sich bei Bedarf ergänzende Informationen erschließen lassen. Zum besseren Verständnis der in den einzelnen Kapiteln beschriebenen Modi Operandi wird empfohlen, die QR-Codes zu Beginn des jeweiligen Kapitels zu nutzen.

1 Die separate Erfassung von Auslandstaten in der PKS wurde zum 01.01.2020 eingeführt. Nach gemeinsamer Evaluation und Abstimmung mit den Bundesländern erfolgte für das Berichtsjahr 2024 erstmalig die Ausweisung der absoluten Zahlen.

Bundeslagebild Cybercrime 2025

Inhalt

1 Cybercrime 2025 – Überblick

Nach einem weiteren Anstieg der Auslandstaten auf 207.888 Fälle übersteigen sie die Straftaten der Inlands-PKS mit 126.034 Fällen deutlich.

333.922

Gesamtfallzahl Cybercrime-Delikte

KI wird zunehmend für cyberkriminelle Aktivitäten genutzt.

1.041

Ransomware-Angriffe wurden deutschlandweit angezeigt.

15,5 Mio. $

Die Ransomware-Zahlungen in Deutschland liegen bei umgerechnet 15.515.377 Mio. US-Dollar.

36.706

DDoS-Angriffe im Netz der DTAG gemessen (+25 %).

mehr als **700**

Angriffsankündigungen und -meldungen durch hacktivistische Akteure auf Ziele in Deutschland.

202.400.000.000 €

Der durch den Bitkom e. V. festgestellte Schaden durch Cyberattacken beträgt 202,4 Mrd. Euro.

1.1 Bedrohungslage

KI

Cyberakteure können mithilfe von künstlicher Intelligenz (KI) die Effizienz, Effektivität und Schnelligkeit ihrer Angriffsmodi verbessern. Die Entwicklungen wirken sich auf alle Phänomenbereiche der Cybercrime aus.

SPAM

Phishing

Aufgrund seiner simplen, aber effektiven Funktionsweise ist Phishing weiterhin ein beliebter Eintrittsvektor.

Die Verbraucherschutzzentrale NRW verzeichnete in Deutschland 382.470 Phishing-Mails. Dies stellt zwar einen Rückgang um ca. 10 % im Vergleich zu 2024 dar, dennoch blieb die Anzahl der verzeichneten Phishing-Mails auf einem hohen Niveau.

Malware

Malware ist das Standardwerkzeug vieler Cyberkrimineller. Neben Droppern bzw. Loadern kommt insbesondere Remote Access Tools und Infostealern eine große Relevanz zu, da diese regelmäßig im Vorfeld von Ransomware-Angriffen eingesetzt werden.

Ransomware

Angriffe mit Verschlüsselungstrojanern sind eine zentrale Bedrohung für Unternehmen und öffentliche Einrichtungen.

2025 wurden 1.041 solcher Angriffe zur Anzeige gebracht, 10 % mehr als im Vorjahr.

Polizeiliche Kriminalstatistik

Bei der zusammengefassten Betrachtung der Inlands- und Auslands-PKS ergibt sich mit 333.922 Fällen ein geringfügiger Anstieg von 0,2 %. Zudem ist weiterhin von einem hohen Dunkelfeld auszugehen.

Ziele und Schäden

Die Zielauswahl krimineller Akteure erwies sich auch 2025 als äußerst heterogen. Die in Deutschland durch Cyberattacken entstandenen Schäden betrugen gemäß einer im Jahr 2025 durchgeführten Erhebung des Bitkom e. V. ca. 202 Mrd. Euro. Im Vergleich zum Vorjahr sind sie damit erneut deutlich angestiegen (+24 Mrd. Euro). Gemessen an den vom Bitkom e.V. ermittelten Gesamtschäden für die deutsche Wirtschaft (289 Mrd. Euro) machten Cyberangriffe ca. 70 % aus.

DDoS und Hacktivismus

Der Trend der letzten Jahre setzt sich fort: 2025 konnte ein signifikanter Anstieg an Überlastungs-Angriffen (+25 %) und hacktivistischen Angriffsankündigungen und -meldungen (+224 %) verzeichnet werden.

Schwachstellen

IT-Schwachstellen stellen kritische Eintrittsvektoren für Cyberangriffe dar.

Laut der US-amerikanischen Behörde CISA (Cybersecurity and Infrastructure Security Agency) wurden 245 Schwachstellen aktiv durch Cyberkriminelle ausgenutzt, ein Anstieg von ca. 32 % im Vergleich zum Vorjahr.

Underground Economy

Die Underground Economy ist Basis nahezu aller cyberkriminellen Handlungen. Von ihr geht eine dauerhaft hohe Bedrohung aus. Dort angebotene Waren und Dienstleistungen nehmen eine zentrale Rolle im Phänomenbereich ein.

1.2 Bedeutende Entwicklungen

JANUAR

Ransomware-Angriff auf das Fraunhofer-Institut für Arbeitswirtschaft und Organisation. Dabei wurde die Ransomware Akira eingesetzt.

FEBRUAR

Inhalte einer Interpol-Datenbank wurden in einem Forum der Underground Economy zum Download angeboten.

Computersabotage zum Nachteil einer Biogasanlage in Niedersachsen durch die pro-russische hacktivistische Gruppierung Z-Pentest-Alliance. Es kam zu Schäden in Höhe von fast 36.000 Euro.

Quelle: LKA Niedersachsen

MÄRZ

Cyberangriff auf die IT-Systeme der Stadtwerke Schwerte, die mittels der Ransomware Nitrogen verschlüsselt wurden.

Quelle: LKA Nordrhein-Westfalen

Kompromittierung von Benutzerkonten der Bundesagentur für Arbeit, bei der die Kontoverbindungen für Leistungsauszahlungen verändert wurden.

Quelle: LKA Bayern

APRIL

Weitere Angriffswellen durch den hacktivistischen Akteur NoName057(16) gegen Ziele in Deutschland. Als Begründung wurde die mögliche Lieferung von Taurus-Marschflugkörpern an die Ukraine angeführt.

MAI

Ransomware-Angriff auf die Deutsche Welthungerhilfe e.V. durch die Tätergruppierung Rhysida. Die Angreifer kopierten Daten aus den betroffenen Systemen vor der Verschlüsselung, veröffentlichten diese anschließend in Auszügen im Darknet und stellten eine Lösegeldforderung in Höhe von 1,8 Mio. Euro.

Quelle: LKA Nordrhein-Westfalen

JUNI

Cyberangriff auf die Media Broadcast Satellite GmbH durch die Ransomware-Gruppierung Qilin. Dabei will die Gruppierung nach eigenen Angaben 870 GB an Daten exfiltriert haben.

JULI

Zahlreiche Angriffe auf Ziele in Deutschland durch NoName057(16) als Reaktion auf strafprozessuale Maßnahmen gegen die kriminelle Gruppierung. Die Anzahl überschritt dabei innerhalb kürzester Zeit das bisher festgestellte Angriffsaufkommen des Akteurs. Die Auswirkungen der Angriffe mit Vergeltungscharakter blieben allerdings unterhalb eines signifikanten Niveaus.

AUGUST

Cyberangriff auf die Gemeinde Hoppegarten/Brandenburg. Rathaus und Bürgerdienste waren als Folge des Angriffs wochenlang gestört.

SEPTEMBER

Ransomware-Angriff auf den IT-Dienstleister Collins Aerospace führte zu Störungen an diversen europäischen Flughäfen. Die Wiederherstellung der Systeme dauerte mehrere Tage an. Dies führte an den betroffenen Flughäfen, darunter London Heathrow, Berlin, Brüssel und Dublin, tagelang zu erheblichen Einschränkungen im Flugverkehr.

OKTOBER

Ein Ransomware-Angriff auf die Stadtwerke Clausthal-Zellerfeld erforderte die Abschaltung der Telefon- und Internetverbindungen. Die Versorgungssicherheit mit Strom, Wasser und Gas war nicht gefährdet.

NOVEMBER

Cyberangriff auf die Stadtwerke Detmold durch die Tätergruppierung crYpt. Infolge des Angriffs waren zentrale IT-Systeme des Energie- und Wasserversorgers zeitweise nicht mehr verfügbar. Die Versorgungssicherheit war gewährleistet.

DEZEMBER

Ransomware-Angriff auf die IDEAL Versicherungsgruppe durch Akira. Die IT-Systeme wurden vorsorglich vom Netz genommen.

2 Polizeiliche Kriminal-statistik

Die PKS dient als polizeiliche Datenbasis für Trendaussagen zur Entwicklung des Phänomenbereichs. Die cyberspezifischen Delikte der CCieS werden in der PKS unter dem Summenschlüssel Cybercrime zusammengefasst. Bei der zusammenhängenden Betrachtung dieser Fallzahlen von Inlands- und Auslands-PKS (Gesamtzahl 333.922) ergibt sich ein geringfügiger Anstieg von 0,2 % im Vergleich zum Vorjahr und somit eine nahezu gleichbleibend hohe Kriminalitätsbelastung im Bereich Cybercrime.

Der seit 2022 verzeichnete rückläufige Trend an Cybercrime-Delikten, bei denen der Handlungsort der Täter im Inland (Inlands-PKS) liegt, setzt sich 2025 mit 126.034 verzeichneten Fällen (-4,1 %) weiter fort.[2] Sowohl die Aufklärungsquote (31,4 %) als auch der Anteil von Cybercrime-Delikten an den registrierten Straftaten insgesamt (2,3 %) verblieb 2025 auf Vorjahresniveau.

Mit einem weiteren Anstieg auf 207.888 Fälle (ca. +3 %) sind im Phänomenbereich Cybercrime erneut erheblich mehr Auslands- als Inlandstaten erfasst. Unter den Auslandstaten werden die Fälle registriert, bei denen der Aufenthaltsort der Täter unbekannt ist oder diese sich nicht in Deutschland aufhalten und ein Schaden/Taterfolg in Deutschland eingetreten ist (siehe Abbildung 1).

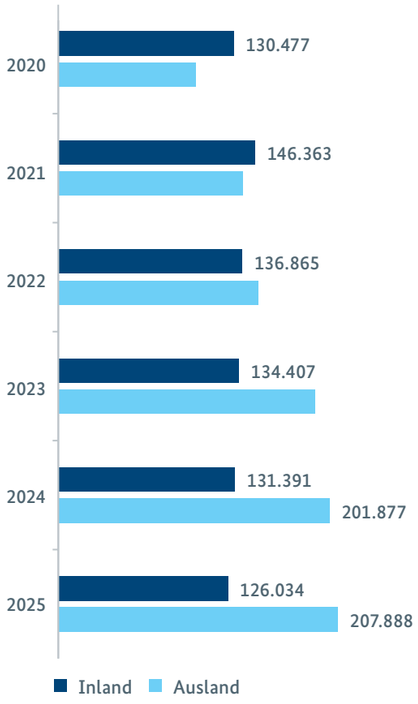

Abbildung 1: Erfasste Cybercrime-Fälle in Deutschland ohne Nennung der absoluten Zahlen bei den Auslandstaten für die Jahre 2020-2023.

2 Obwohl die Fallzahlen der Inlands-PKS für das Jahr 2025 leicht rückläufig sind, ist dies kein Indiz für einen generellen Rückgang der registrierten Cyberstraftaten mit Auswirkungen auf Deutschland. Die Inlands-PKS hat hier nur eine begrenzte Aussagekraft, da vielfach das Agieren der Tatverdächtigen nicht im Inland verortet werden kann. Ein realistischeres Bild der Kriminalitätsbelastung anhand der PKS ergibt sich erst bei der Betrachtung dieser Fallzahlen in Verbindung mit den Auslandstaten.

Cybercrime macht fast ein Drittel aller Fälle der Auslands-PKS aus.

Vergleicht man den Anteil an Cybercrime-Delikten der Inlands- und Auslands-PKS, wird die hohe Relevanz der Auslandstaten für diesen Deliktsbereich deutlich: Während Cybercrime-Delikte in der Inlands-PKS nur einen Anteil von 2,3 % an den Gesamtstraftaten darstellen, machen sie in der Auslands-PKS beinahe ein Drittel aller dort erfassten Taten aus (31,4 %, siehe Abbildung 2).

Der hohe Anteil an Fällen, bei denen der Handlungsort der Tatverdächtigen nicht im Inland verortet werden kann, stellt die ermittelnden Polizeibehörden vor große Herausforderungen. Dies spiegelt sich weiterhin in einer sehr niedrigen Aufklärungsquote (2,0 %) der in der Auslands-PKS dargestellten Fallzahlen der Cybercrime wider.[3]

Die Fallzahlen zum Straftatbestand § 127 StGB „Betreiben krimineller Handelsplattformen im Internet“ werden nicht vom Summenschlüssel Cybercrime umfasst. Die Fallzahl erhöhte sich 2025 leicht auf 93 (vgl. 2024: 92 Fälle). Die Aufklärungsquote hat sich dabei verdoppelt; insgesamt konnten 24,7 % dieser Fälle aufgeklärt werden. Es muss hierbei allerdings berücksichtigt werden, dass aufgrund der niedrigen Grundgesamtheit der Fallzahlen eine Zu- bzw. Abnahme aufgeklärter Fälle stark ins Gewicht fällt.

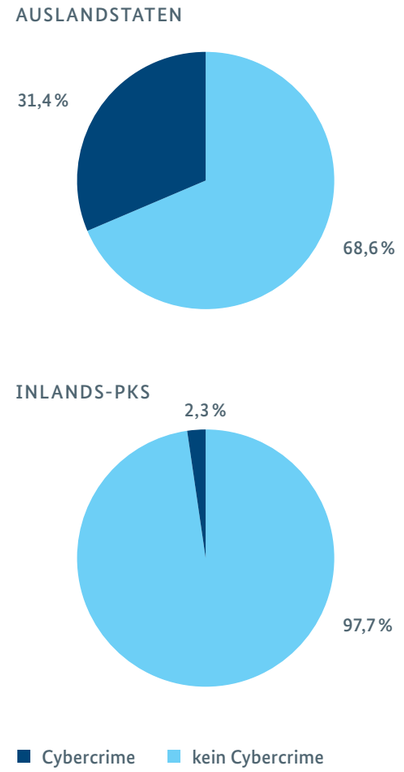

Abbildung 2: Anteil von Cybercrime-Delikten an Inlands- und Auslandstaten (gesamt).

Die Kriminalitätsbelastung durch Cybercrime bleibt auf einem hohen Niveau.

3 Generell gilt innerhalb der PKS ein Fall dann als aufgeklärt, wenn nach dem polizeilichen Ermittlungsergebnis die rechtmäßigen Personalien von mindestens einem Tatverdächtigen bekannt sind. Juristische Hürden und mangelnde Kooperationsbereitschaft im Ausland können gerade diese Täteridentifizierung und Strafverfolgung erschweren oder sogar verhindern, sodass selbst vorliegende vielversprechende Ermittlungsansätze die Aufklärungsquote nicht verbessern.

3 Bedrohungen im Fokus

3.1 Ransomware & Data Extortion

1.041 Angriffe wurden zur Anzeige gebracht.

96 % der Angriffe richteten sich gegen Unternehmen, Organisationen und Institutionen.

Häufigste Ransomware-Varianten

1. Akira
2. SafePay
3. INC/Lynx
4. LockBit
5. Qilin
6. DragonForce
7. Medusa Locker
8. Sarcoma
9. Makop
10. RansomHub

ca. 90 % der Angriffe richteten sich gegen kleine und mittlere Unternehmen (KMU).

ca. 100 Ransomware-Varianten wurden gegen deutsche Geschädigte eingesetzt.

Nur **7 %** der Geschädigten zahlten Lösegeld.

ca. 76 % aller Ransomware-Angriffe konnten dem Modus Operandi Double Extortion zugeordnet werden.

Im Mittel gezahlt wurden umgerechnet: ca. 456.335 US-Dollar

Abbildung 3: Kennzahlen zu Ransomware-Angriffen in Deutschland im Jahr 2025. Die Informationen basieren auf einer Erhebung des BKA in den Bundesländern und den zuständigen BKA-Fachdienststellen. Alle hier berichteten Zahlen der bundesweiten Fallerhebung berücksichtigen nur diejenigen Fälle, bei denen Informationen zu den jeweiligen Kategorien vorlagen. Fälle mit Angaben „unbekannt" oder ohne Angaben wurden hier nicht berücksichtigt. Alle Angaben zu Lösegeldern, die sich aus der Fallerhebung ergeben, wurden für eine internationale Vergleichbarkeit in US-Dollar umgerechnet.

Angriffe mit Verschlüsselungstrojanern stellten 2025 erneut eine herausfordernde Bedrohung für Unternehmen dar. Mit 1.041 angezeigten Fällen wurde ein Anstieg um 10 % im Vergleich zum Vorjahr verzeichnet (2024: 950 Fälle).

Die Ransomware-Angriffe erfolgten in Wellen über das Jahr verteilt. Besonders viele Angriffe fanden in den Monaten März, Juli und Oktober statt, womit der bislang häufig beobachtete Angriffsrückgang in den Sommermonaten ausblieb (siehe Abbildung 4).

Auf sogenannten Dedicated Leak Sites (DLS) werden mutmaßlich geschädigte Unternehmen für „naming and shaming" namentlich von den Tätern aufgelistet und ggf. ihre gestohlenen Daten veröffentlicht. Diese Vorgehensweise wird sowohl für Double Extortion als auch für Data Extortion angewandt. Eine für 2025 durchgeführte Analyse der veröffentlichten Daten[4] bestätigt den starken Anstieg an Ransomware-Angriffen, den auch die Daten der polizeilichen Fallerhebung zeigen. Insgesamt wurden von den Tätern 292 (+88 %) deutsche Geschädigte gelistet.

Auch im Bereich der Lösegeldzahlung gab es deutliche Entwicklungen. Die Zahlungsbereitschaft von Geschädigten sank. In der bundesweiten Fallerhebung gaben nur 7 % (2024: 9 %) der Geschädigten von Ransomware-Angriffen an, Lösegeld gezahlt zu haben.[5] Weltweit zahlten nach Daten des IT-Dienstleisters Coveware hingegen durchschnittlich 24 % der angegriffenen Unternehmen (2024: 30 %, Abbildung 5).[6] Die Lösegeldzahlung bei Verschlüsselung scheint weiterhin von vielen Geschädigten lediglich als letzte Möglichkeit genutzt zu werden, wenn die eigenen Daten nicht mehr anders wiederhergestellt werden können.

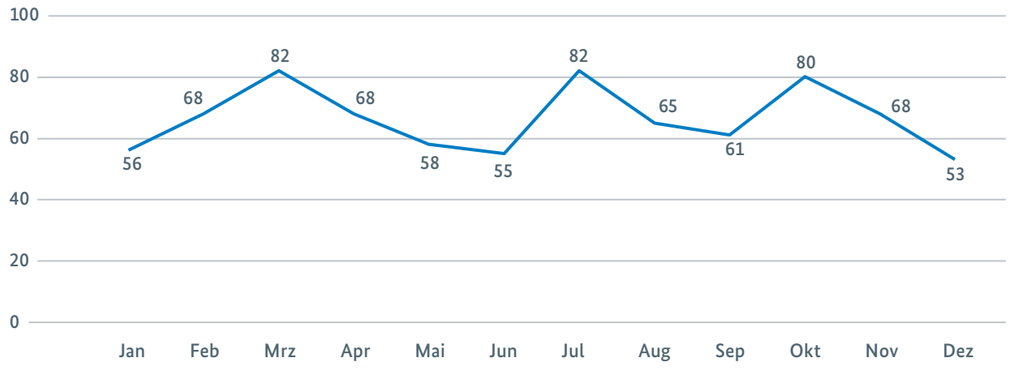

Abbildung 4: Bundesweite Erhebung polizeilich bekannt gewordener Ransomware-Angriffe im Jahr 2025. Die abgebildeten Daten umfassen ausschließlich das polizeiliche Hellfeld.

4 Auf der Internetseite eCrime.ch werden Daten zu Unternehmen bereitgestellt, die Ziel von Data Extortion und Double Extortion Angriffen wurden und öffentlich auf aktiven DLS erpresst werden. Stand 14.04.2026. Zahl kann retrograden Anpassungen unterliegen.

5 Angabe für Fälle, in denen eine Angabe zur Lösegeldzahlung gemacht wurde, n= 613.

6 Coveware (2025 und 2026). Quartalsberichte 2025. Online abrufbar unter *https://www.coveware.com/ransomware-quarterly-reports*

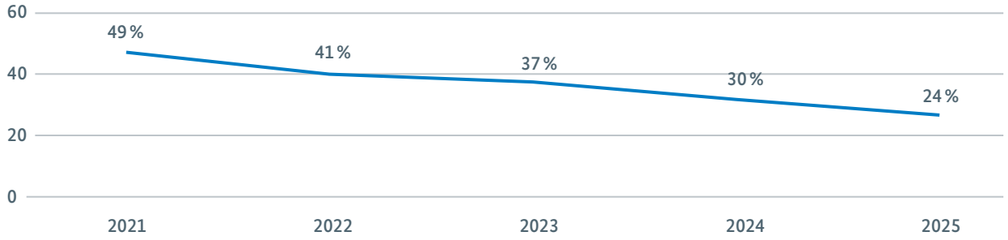

Abbildung 5: Anteil an Unternehmen, die nach einem Ransomware-Angriff Lösegeld gezahlt haben.
Quelle: Coveware (2025 u. 2026). Quartalsberichte 2025.

Bei den Geschädigten, die Lösegeld zahlten, war der durchschnittliche Betrag höher als im Vorjahr. Bezogen auf Deutschland konnte im Rahmen der bundesweiten Fallerhebung ein deutlicher Anstieg von 65 % der Höhe der durchschnittlichen Lösegeldzahlungen festgestellt werden. So wurden im Mittel umgerechnet 456.335 US-Dollar von deutschen Unternehmen an Ransomware-Gruppierungen gezahlt, 2024 waren es noch 276.615 US-Dollar. Die Betrachtung der insgesamt gezahlten Lösegeldsumme zeigt mit 15,5 Mio. US-Dollar zudem eine erhebliche Steigerung um 93 % (siehe Abbildung 6).

Weltweit stellte Coveware bei seiner Kundschaft eine durchschnittliche Lösegeldzahlung von 662.944 US-Dollar fest. Dies entspricht einem Anstieg von 47 % zum Vorjahr.[7] Chainalysis, die Kryptowallets der Akteure analysieren, sahen in ihren Daten zu durchschnittlichen Lösegeldzahlungen sogar einen Anstieg um 368 %.[8] Trotz erheblich gestiegener durchschnittlicher Lösegeldzahlungen war die Summe aller weltweiten Lösegeldtransaktionen auf bekannten Kryptowallets von Ransomware-Akteuren im Vergleich zum Vorjahr nahezu gleichbleibend, da insgesamt weniger Zahlungen erfolgten.[9] Um ihre illegalen Gewinne zu stabilisieren bzw. auf diesem hohen Niveau zu halten, müssen Ransomware-Akteure, aufgrund der sinkenden Zahlungsbereitschaft der Betroffenen, sowohl mehr Angriffe durchführen als auch höhere Forderungen stellen.

In Deutschland gezahlte Lösegelder:

15.515.377 US-Dollar

Summe aller in der Ransomware-Fallerhebung erfassten Lösegeldzahlungen

> 800 Mio. US-Dollar

Festgestellte Lösegeldzahlungen auf Kryptowallets von Ransomware-Akteuren weltweit

Abbildung 6: Summe der in Deutschland gezahlten Lösegelder. Quelle: Ransomware-Fallerhebung (links)
Einnahmen durch weltweite Ransomware-Angriffe. Quelle: Chainalysis (2026). The 2026 Crypto Crime Report. (rechts)

7 Coveware (2025 und 2026).Quartalsberichte 2025. Online abrufbar unter *https://www.coveware.com/ransomware-quarterly-reports*

8 Die Auswertung erfolgte durch das Blockchain-Analyse-Unternehmen Chainalysis. Quelle: Chainalysis (2026). The 2026 Crypto Crime Report.

9 Die Auswertung erfolgte durch das Blockchain-Analyse-Unternehmen Chainalysis. Quelle: Chainalysis (2026). The 2026 Crypto Crime Report.

Neben Ransomware-Angriffen bildet sich Data Extortion immer mehr als alternativer Modus Operandi heraus. In diesen Fällen lag die Zahlungsbereitschaft der Geschädigten 2025 weltweit im Schnitt bei 29 %, während sie 2024 noch bei 34 % lag. Obwohl auch hier seit mehreren Jahren ein rückläufiger Trend zu beobachten war, fiel dieser weniger stark aus als bei Angriffen mit Verschlüsselungstrojanern.[10]

Data Extortion: Die Evolution zu WorldLeaks

2021 trat die Ransomware HIVE erstmalig in Erscheinung und galt als eine der weltweit aktivsten Varianten. Nach polizeilichen Maßnahmen gegen die Infrastruktur der dahinterstehenden Gruppierung im Zuge der Operation Dawnbreaker stellte sie 2023 ihre Aktivitäten ein. Im selben Jahr trat die Gruppierung Hunters International in Erscheinung. Große Übereinstimmungen mit HIVE legten nahe, dass es sich um deren Nachfolger (sogenanntes Rebranding) handelte. Zwei Jahre später beendete die Gruppierung ihre Ransomware-Aktivitäten und stellte ein neues Projekt namens WorldLeaks vor, das seit Mai 2025 aktiv ist. Seit dem Wechsel verfolgt die Gruppierung einen neuen Modus Operandi: Sie verschlüsselt keine Daten mehr, distanziert sich aktiv von Ransomware-Angriffen und fokussiert sich stattdessen auf die Ausleitung von Daten und die Erpressung mit deren Veröffentlichung (Data Extortion).

Data Extortion gewinnt zunehmend an Bedeutung.

Ransomware-Varianten und -Gruppierungen unterliegen schon seit dem Aufkommen des Phänomenbereichs einem konstanten Wandel. Aus verschiedenen Gründen, wie internen Differenzen oder externem Druck, verschwinden auch etablierte Varianten „vom Markt“, während neue in Erscheinung treten. Nationale und internationale operative Maßnahmen sowie Sanktionen gegen Ransomware-Gruppierungen und ihre Infrastruktur stören die weltweiten Ransomware-Aktivitäten. Die Disruptionen in der Ransomware-Landschaft, die 2024 größere Ransomware-Gruppierungen wie Phobos und LockBit betrafen, setzten sich auch 2025 fort. Durch polizeiliche Maßnahmen gegen 8Base und BlackSuit konnten deren Aktivitäten unterbunden werden. Die Gruppierung BlackBasta stellte ihre Tätigkeit aufgrund interner Streitigkeiten ein. Es zeigte sich, dass die dadurch entstandene Lücke in der Ransomware-Szene 2025 überwiegend durch die in Deutschland besonders aktiven Gruppierungen Akira und SafePay genutzt wurde.

Die Anzahl der Ransomware-Angriffe und die Höhe der Lösegeldzahlungen in Deutschland steigen erheblich.

10 Coveware (2025 und 2026). Quartalsberichte 2025.Online abrufbar unter *https://www.coveware.com/ransomware-quarterly-reports*

3.2 Distributed Denial-of-Service (DDoS) & Hacktivismus

36.706
Angriffe im Jahr (+25 %)

Ø 3.059
Angriffe pro Monat (+25 %)

Ø Dauer eines Angriffs (-15 %)
41 Minuten

Ø Bandbreite (-41 %)
705 MBit/s

Häufigste Angriffsziele

- (Bundes-)Behörden
- Öffentliche Verwaltungen
- Verkehrsunternehmen
- Logistikdienstleister

Mehr Hacktivismus

Über 700
Angriffsankündigungen und -meldungen auf Ziele in Deutschland

+224 % ↗
im Vergleich zum Vorjahr

Abbildung 7: Zahlen und Fakten zur DDoS-Lage 2025 in Deutschland. Quelle der Angriffsparameter: Deutsche Telekom AG.

Die Relevanz von Überlastungsangriffen nahm 2025 weiter zu. Nach Angaben der Deutschen Telekom AG wurden 2025 über 36.000 DDoS-Angriffe auf Ziele im Netz des IT-Dienstleisters erfasst (Vergleich zu 2024: 29.399 DDoS-Angriffe/+25 %). Durchschnittlich wurden über 3.000 DDoS-Angriffe pro Monat verzeichnet (siehe Abbildung 8).

Ein Anstieg an DDoS-Angriffen ist auch auf europäischer Ebene sichtbar: Der IT-Sicherheitsdienstleister Link 11 verzeichnete einen Anstieg von über 75 % im Vergleich zum Vorjahr. Als Gründe werden hierfür die Zunahme von hacktivistischen Aktivitäten im geopolitischen Kontext, aber auch der zunehmende Einsatz von Automatisierungen und KI, die hohe Anzahl ungeschützter internetfähiger Geräte (Internet-of-Things/IoT) sowie ein effizienteres Management von Botnetzen durch Cyberkriminelle und Stresser-Dienste angeführt.

Das Angriffsaufkommen von DDoS-Angriffen steigt seit 2023 sowohl auf deutscher als auch auf europäischer Ebene kontinuierlich an. Damit stellen solche Angriffe eine konstante, in ihrer Quantität jedoch stetig ansteigende Bedrohung für Unternehmen und auch Behörden dar. Obwohl Angriffsbandbreite und -dauer gesunken sind, ist dies nicht gleichzusetzen mit einer sinkenden Bedrohungslage: Die Reduzierung dieser Parameter bei gleichzeitigem Anstieg der Fallzahlen deutet auf eine große Menge an Angriffen mit niedriger Bandbreite hin, die allerdings in kürzerer Zeit ihre Wirkung entfalten können.

Der Ausbau von Botnetzen führt zu einem erhöhten Bedrohungspotenzial durch DDoS-Angriffe.

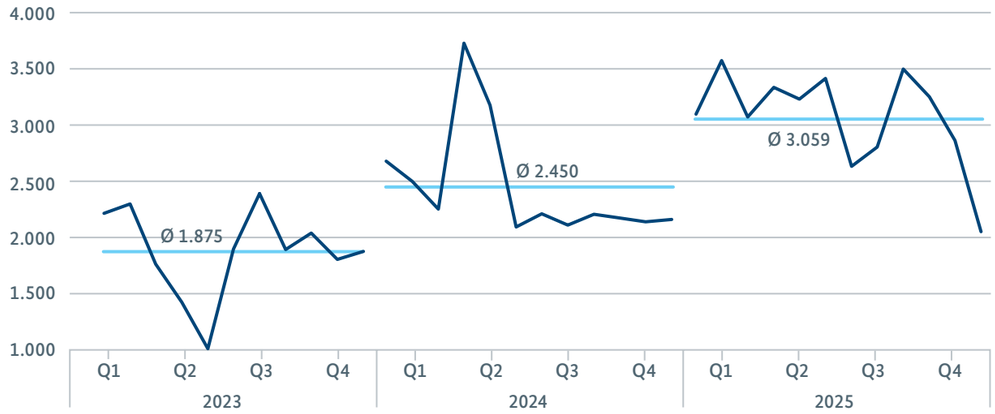

Abbildung 8: Anzahl an DDoS-Angriffen in den Netzen der DTAG für die Jahre 2023 bis 2025.

DDoS-Angriffe sind auch der bevorzugte Modus Operandi von hacktivistischen Akteuren, deren Aktivitäten 2025 ebenfalls zunahmen. Diese Akteure begleiten ihre Aktivitäten öffentlichkeitswirksam unter anderem mit Beiträgen auf X oder speziellen Telegram-Kanälen. Aus dem Monitoring dieser Angriffsankündigungen und -meldungen ergibt sich in der Gesamtbetrachtung ein Zuwachs um 224 % bei Aktivitäten gegen Ziele in Deutschland.[11]

Die hier aktivste hacktivistische Gruppierung NoName057(16) hat ihre Kampagnen auf deutsche Ziele mit insgesamt 10 DDoS-Angriffswellen 2025 nahezu verdoppelt (2024: 6). Waren 2024 noch 137 Behörden und Unternehmen von Überlastungsangriffen der Gruppierung betroffen, so stieg diese Zahl 2025 erheblich auf 378 Betroffene an (+176 %). In der Propaganda der Täterschaft wird hauptsächlich die kontinuierliche politische Unterstützung Deutschlands für die Verteidigung der Ukraine gegen den russischen Angriffskrieg als Anlass für die regelmäßigen DDoS-Angriffe genannt. Zudem reagierte die Gruppierung kurzzeitig mit vergeltungsorientierten Überlastungsangriffen auf die wirkungsvolle Intervention des internationalen Ermittlungsverbunds der Operation Eastwood im Sommer 2025. Die Auswirkungen der Angriffe mit Vergeltungscharakter blieben allerdings unterhalb eines signifikanten Niveaus.

Die Aktivitäten hacktivistischer Gruppierungen sind primär darauf ausgerichtet, mediale Aufmerksamkeit zu erreichen und dadurch Einfluss auf politische und gesellschaftliche Entscheidungen in Deutschland zu nehmen. Durch großflächige DDoS-Angriffe, die auf die Nichterreichbarkeit von Webseiten abzielen, wird für die Bevölkerung zunehmend die Vulnerabilität wesentlicher technischer Infrastrukturen im Alltag erkennbar. Wenngleich der Schaden durch DDoS-Angriffe aus technischer Sicht häufig lediglich moderat ausfällt, können sie im Gesamtkontext weiterer hybrider Bedrohungen als erheblich bewertet werden.

Abbildung 9: Screenshot aus Telegram-Kanal von NoName057(16) zur Vergeltungskampagne nach Operation Eastwood.

Geopolitische Konflikte führen in Deutschland zu einem massiven Anstieg an hacktivistischen Kampagnen.

11 BKA-Auswertung.

3.3 Künstliche Intelligenz

KI entwickelt sich kontinuierlich weiter und gewinnt zunehmend an Relevanz für die Cybercrime-Bedrohungslage. Bislang liegen keine polizeilichen Kennzahlen zum konkreten KI-Einsatz in Cybercrimedelikten vor, dennoch sind Veränderungen in der Kriminalitätsentwicklung auch in den verschiedenen Phänomenbereichen der Cybercrime zu beobachten.

Dabei ist KI als solche erst einmal neutral zu bewerten, denn ihr Einsatzzweck hängt vor allem vom jeweiligen Nutzungsmotiv ab: Dieselben Fähigkeiten, die zur Verbesserung der (digitalen) Sicherheit beitragen, können auch für cyberkriminelle Aktivitäten genutzt werden. KI-Entwickler wie OpenAI und Google bestätigen auf Basis ihrer Nutzungsaktivitäten bereits seit 2024, dass ihre Modelle für cyberkriminelle Aktivitäten missbraucht werden.[12]

Der Einsatz von KI senkt die technische Einstiegshürde für jegliche cyberkriminelle Aktivitäten. Aber auch versiertere Cyberakteure können mithilfe von KI die Effizienz, Effektivität und Schnelligkeit ihrer Angriffsmodi verbessern. Die Auswirkungen dieser Entwicklungen sind bei allen Phänomenbereichen der Cybercrime zu beobachten.

KI senkt die technischen Einstiegshürden für Cybercrime.

Durch Automatisierung mittels KI kann sowohl die Erstellung von Phishing-Webseiten als auch der Versand von Phishing-Mails mit deutlich weniger (Zeit-)Aufwand und in deutlich größerem Ausmaß erfolgen, wodurch das Angriffsvolumen zunimmt. Die sprachlichen Fähigkeiten von KI führen außerdem zu fehlerfreien Texten, die zugleich mühelos in verschiedene Sprachen übersetzt werden können. Auch können Darstellung und Kommunikationsstil bekannter Unternehmen glaubhafter imitiert und die Inhalte durch automatisierte Recherche und Sammlung von persönlichen Informationen besser auf die Empfänger zugeschnitten werden. Insgesamt gibt es dadurch weniger Anhaltspunkte für Zweifel an der Authentizität.

Phishing-Mails wirken durch KI authentischer und sind dadurch gefährlicher.

KI kann auch missbraucht werden, um ein Zielsystem strategisch auszukundschaften (sogenannte Reconnaissance), Schwachstellen zu identifizieren und sich somit schneller und unauffälliger Zugang zu verschaffen.

Schwachstellen sind durch KI leichter zu identifizieren und auszunutzen.

12 OpenAI (01.10.2025). Disrupting malicious uses of AI: an update. Online abrufbar unter: *https://cdn.openai.com/threat-intelligence-reports/7d662b68-952f-4dfd-a2f2-fe55b041cc4a/disrupting-malicious-uses-of-ai-october-2025.pdf*; Google Threat Intelligence Group (29.01.2025). Adversarial Misuse of Generative AI. Online abrufbar unter: *https://cloud.google.com/blog/topics/threat-intelligence/adversarial-misuse-generative-ai*

Im Rahmen der Softwareentwicklung kann Vibe Coding[13] bei unvorsichtiger Nutzung eine Vielzahl von Sicherheitsrisiken bergen. Das gilt vor allem dann, wenn Software vollständig mit KI geschrieben wird, da hierdurch auch unsichere oder potenziell schadhafte Software-Bausteine übernommen werden können. Doch auch Cyberkriminelle machen sich KI-Codingfähigkeiten zunutze. So taucht zunehmend Schadcode auf, bei dem eine KI-Nutzung mindestens vermutet wird.

Malware-Varianten mit KI

Im Juli 2025 warnte das ukrainische Computer Emergency Response Team (CERT-UA) vor einer Malware namens **Lamehug**, die während des Angriffs mit einem externen KI-Modell interagiert. Dieses nimmt die Anweisungen der Malware entgegen und generiert dann dynamisch auf dem Opfersystem ausführbare Befehle, mit denen Informationen über das System gesammelt, lokale Dokumente durchsucht, kopiert und ggf. ausgeleitet werden.[14] Mit **Promptlock** wurde kurz darauf durch einen Sicherheitsdienstleister eine weitere Malware entdeckt, die während Cyberangriffen mit einem KI-Sprachmodell interagiert.[15] Weitere Sicherheitsdienstleister berichten von einer neuen hartnäckigen und anpassungsfähigen Malware namens **Koske**, die zum Schürfen von Kryptowährungen auf Linux-Systemen entwickelt wurde, oder von Malware-Varianten wie **Promptflux**, die ihren eigenen Code bei jeder Infektion oder Ausführung automatisch umwandeln, um von signaturbasierten Anti-Viren-Systemen nicht wiedererkannt zu werden.[16]

Auch bei Ransomware-Angriffen werden KI-Fähigkeiten angewendet. So können die enormen Datenanalysefähigkeiten vor, während und nach einem Angriff missbraucht werden, um die unzähligen Elemente eines Systems zu strukturieren und zu analysieren. Dadurch können aus der breiten Masse die besonders sensiblen Dateien und Informationen herausgefiltert werden und Angreifer länger unbemerkt bleiben. Zudem werden die generativen KI-Fähigkeiten durch Ransomware-Akteure missbraucht, um Informationen zu ihren Angriffszielen zu sammeln, Phishing-Mails zu erstellen, Malware zu verbessern und Täter-Opfer-Kommunikation zu übersetzen.

KI erleichtert die Durchführung von Cyberangriffen – die Angriffsquantität und -qualität steigt.

13 Vibe Coding bezeichnet KI-gestützte Softwareentwicklung, durch die Nutzende mithilfe einfacher Sprache und gezielter Prompts auch ohne eigene Programmierkenntnisse funktionale Anwendungen erstellen können.

14 CERT-UA (17.07.2025). UAC-0001 cyberattacks on the security and defense sector using the LAMEHUG software tool using the LLM (CERT-UA#16039). Online abrufbar unter: *https://cert.gov.ua/article/6284730*

15 Aqua Security Software Ltd. (24.07.2025). AI-Generated Malware in Panda Image Hides Persistent Linux Threat. Online abrufbar unter: *https://www.aquasec.com/blog/ai-generated-malware-in-panda-image-hides-persistend-linux-threat/*

16 Google Threat Intelligence Group (05.11.2025). GTIG AI Threat Tracker: Advances in Threat Actor Usage of AI Tools. Online abrufbar unter: *https://cloud.google.com/blog/topics/threat-intelligence/threat-actor-usage-of-ai-tools*

Durch den zunehmenden Einsatz von sogenannter agentischer KI bzw. KI-Agents[17] können Cyberdelikte zukünftig in noch höherer Intensität und automatisierter durchgeführt werden, was die Bedrohungslage weiter verschärft.

Cyberangriffe mit Claude

Im September 2025 entdeckte der KI-Entwickler Anthropic eine Angriffsserie, bei der sein KI-Modell Claude missbraucht wurde, um simultan und nahezu autonom ca. 30 Organisationen und Regierungsbehörden anzugreifen. Der Angriff bestand aus mehreren Phasen, darunter unter anderem Auswahl der Ziele, Auskundschaften der Zielsysteme, Suche bzw. Identifikation von Schwachstellen, Validierung von Exploits, Sammeln von Zugangsdaten, Ausweitung von Zugriffsrechten und Ausleitung von Daten. Claude fungierte hierfür als zentrales Koordinierungstool, das unter anderem komplexe mehrstufige Angriffsschritte in unauffälligere Teilaufgaben unterteilte. Dabei wurden die Prompts an die KI so formuliert, dass sie – jede für sich betrachtet – wie legitime technische Nutzeranfragen wirkten. Zusätzlich entwickelten die Angreifer eine Methode, um die Cyberangriffe weitestgehend ohne direkte menschliche Beteiligung ausführen zu können. Diese war nur noch punktuell erforderlich, z. B. bei der Autorisierung der Ausführung von Exploits.

Je besser KI-Tools werden, desto stärker werden sie genutzt und in organisationale IT-Infrastrukturen eingebunden. Deshalb werden parallel zunehmend Schwachstellen und Angriffstechniken entwickelt und getestet, die sich auf KI-Systeme fokussieren. Das umfasst z. B. die Kompromittierung der KI-Rechenleistung für cyberkriminelle Aktivitäten oder sogenannte Indirect Prompt Injections, die ein KI-Modell mittels versteckter Prompts zu ungewollten und/oder maliziösen Aktivitäten manipulieren. Der perspektivisch zunehmende Einsatz agentischer KI verschärft auch diese Bedrohungslage, da sie in der Regel mit weitreichenden Befugnissen in der jeweiligen IT-Umgebung ausgestattet sind, die im Falle einer Kompromittierung gezielt missbraucht werden könnten.

KI ist nicht nur Tatmittel, sondern auch Angriffsziel.

17 KI-Agenten gehen über die bloße Ausgabe generierter Inhalte hinaus. Sie können eigenständig Entscheidungen treffen und somit auch komplexe, mehrstufige Aufgaben weitgehend autonom erledigen, vergleichbar mit persönlichen Assistenten.

4 Polizeiliche Maßnahmen

4.1 Zentrale Ermittlungen

Im Phänomenbereich Cybercrime im engeren Sinne treten Straftaten mit gleichartigem Modus Operandi häufig in wellenförmigen Abständen auf. Diese zeichnen sich dadurch aus, dass viele Angriffe durch einen Akteur innerhalb eines eng umgrenzten zeitlichen Rahmens begangen werden. Dabei gibt es keinen feststellbaren örtlichen Schwerpunkt, stattdessen finden die Straftaten länderübergreifend oder sogar bundesweit statt. Die Cybercrime-Dienststellen in Deutschland setzen diesen Straftatenwellen sogenannte Zentrale Ermittlungen entgegen. Bei diesen koordinierten Bund-Länder-Verfahren übernimmt eine Polizeidienststelle oder ein Verbund von Dienststellen die federführende Ermittlungstätigkeit unter staatsanwaltschaftlicher Sachleitung. Ziel ist eine gesammelte Spurenbearbeitung, insbesondere zur Vermeidung von Doppelermittlungen und zur Ressourcenschonung, ohne dabei für gleichartige – bei anderen Polizeidienststellen im Bundesgebiet vorliegende – Ermittlungsverfahren eine formale Zuständigkeit zu begründen.

Zentrale Ermittlungen bewirken eine effektivere Strafverfolgung.

Neben der Koordination der zentralen Ermittlungen und der Unterstützung der Länderverfahren bei vorliegenden internationalen Bezügen, übernimmt das Bundeskriminalamt bei ausgewählten Sachverhalten auch selbst die zentrale Ermittlungsführung. Dieses zwischen Land und Bund abgestimmte Vorgehen bei bedeutsamen nationalen Fällen ermöglicht eine effektive bundesweite Strafverfolgung im Bereich Cybercrime.

34 Zentrale Ermittlungen bundesweit (2024: 25)

BKA **5**

LKA **29** Länderdienststellen

29 gegen Ransomware-Akteure (2024: 22)

2 gegen Data Extortion-Akteure (2024: 1)

2 im Bereich DDoS (2024: 2)

SPAM **1** gegen Anbieter von Phishing-Kits (2024: 0)

Abbildung 10: Zahlen und Fakten zu Zentralen Ermittlungen 2025 in Deutschland.

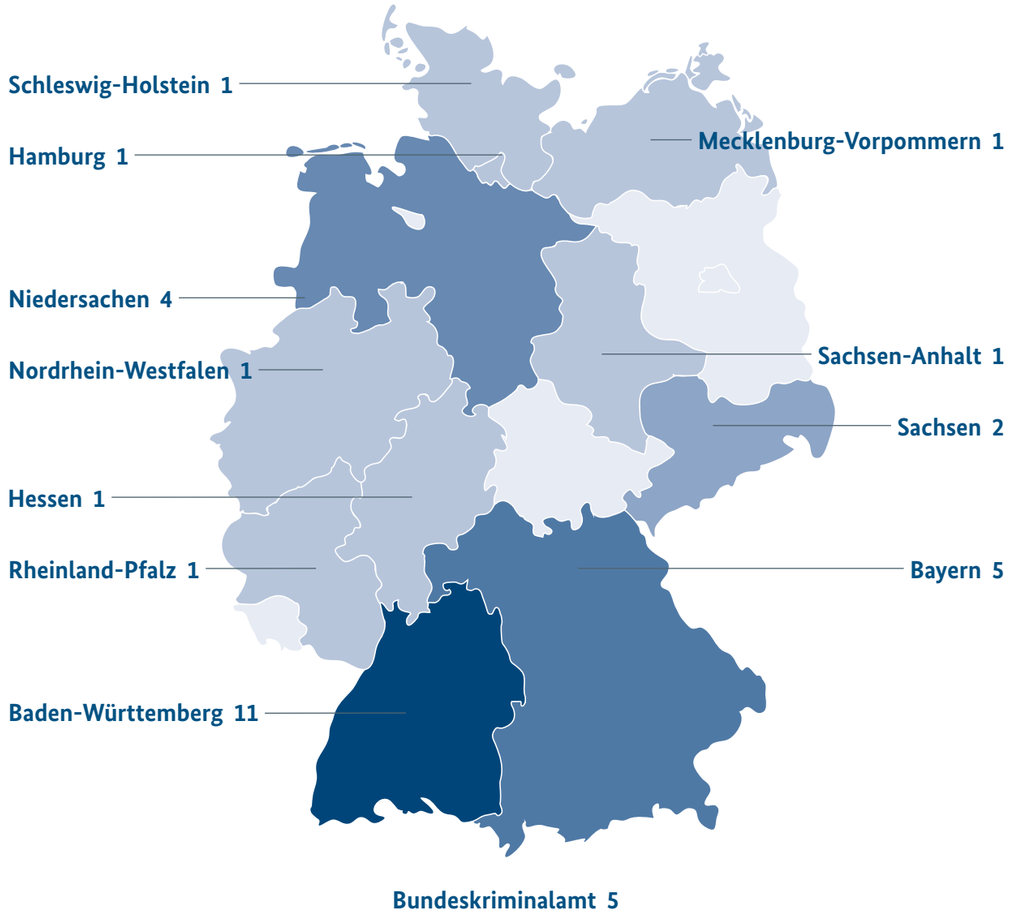

Abbildung 11: Zentrale Ermittlungen 2025 in Deutschland nach Bundesländern.

Fallbeispiel: Zentrale Ermittlungen gegen SafePay

Das LKA Rheinland-Pfalz führt seit April 2025 die zentralen Ermittlungen gegen die Ransomware Gruppierung SafePay. Weltweit sind mindestens 425 Institutionen von SafePay betroffen, Schwerpunkte liegen in den USA und Deutschland. Bundesweit sind mindestens 86 Fälle bekannt. Seit Übernahme der zentralen Ermittlungen konnten bislang 30 Serversicherungen zu Beweiszwecken durchgeführt werden. Durchgeführte technische Maßnahmen ergaben Hinweise auf die genutzte Serverinfrastruktur, die möglicherweise auf russische Reseller hindeuten.

Quelle: LKA Rheinland-Pfalz

4.2 Operative Erfolge

2025 war geprägt von intensiven Ermittlungsarbeiten und zahlreichen Maßnahmen der nationalen und internationalen Strafverfolgungsbehörden. Diese richteten sich gegen sämtliche Bereiche der Cyberkriminalität im engeren Sinne, darunter illegale Marktplätze und Dienstleister der Underground Economy, Krypto-Exchange-Services sowie die Infrastruktur diverser Cybercrime-Akteure. Dabei stellten Strafverfolgungsbehörden Vermögenswerte im dreistelligen Millionenbereich sicher.

Im Folgenden werden Ermittlungserfolge aus dem Jahr 2025 dargestellt:

Januar: Takedown der kriminellen Handelsplattformen Nulled und Cracked

Die Generalstaatsanwaltschaft Frankfurt am Main – Zentralstelle zur Bekämpfung der Internetkriminalität (ZIT) und das BKA gingen gegen die beiden größten Handelsplattformen für Cybercrime im Internet vor. Hierbei handelte es sich um die Webseiten „nulled.to“ und „cracked.io“, die zusammen insgesamt rund zehn Millionen registrierte Nutzerkonten aufwiesen. Im Rahmen der international abgestimmten Operation Talent wurden insgesamt sieben Durchsuchungsmaßnahmen durchgeführt und unter anderem Server, Accounts und kriminell genutzte Domains in zehn Ländern beschlanahmt sowie die beiden Plattformen abgeschaltet. Zudem wurden seitens der internationalen Partnerdienststellen ein Zahlungsdienstleister sowie ein Hosting-Dienst vom Netz genommen, die unmittelbar zum Wirtschaftsgeflecht der Plattformen gehörten. Auch die IT-Infrastrukturen der kriminellen Plattformen sowie E-Mail-Adressen, IP-Adressen und Kommunikationsverläufe der rund zehn Millionen registrierten Nutzerkonten wurden sichergestellt und sind Grundlage für weitere internationale Ermittlungen gegen kriminelle Verkäufer und Nutzer der Plattformen.

Im Zuge der Ermittlungen wurden insgesamt acht Personen identifiziert, die unmittelbar am Betrieb der kriminellen Handelsplattformen mitgewirkt haben sollen, darunter zwei deutsche Staatsangehörige. Zwei Personen, darunter ein deutscher Staatsangehöriger, wurden festgenommen. Zudem konnten Vermögenswerte im mittleren sechsstelligen Bereich gesichert werden.

Februar: Maßnahmen gegen die Ransomware-Gruppierung 8Base

Bei international konzertierten Maßnahmen gegen Mitglieder der Ransomware-Gruppierung 8Base, deren Angriffe sich auch auf deutsche Ziele richteten, wurden in Thailand vier russische Staatsangehörige aufgrund von Ersuchen des US-amerikanischen Federal Bureau of Investigation (FBI) und des Schweizer Bundesamtes für Polizei festgenommen. Thailändische Behörden durchsuchten die Wohnungen der Beschuldigten. Unter den vier Personen war auch der Administrator der Gruppierung, der zudem Zugriff auf das Administrator-Panel der Ransomware Phobos gehabt haben soll. Darüber hinaus wurden 115 Server durch Maßnahmen der Generalstaatsanwaltschaft (GenStA) Bamberg, Zentralstelle Cybercrime (ZCB), und des Bayerischen LKA beschlagnahmt und mit einem behördlichen Seizure-Banner versehen.

März: Takedown der Kryptowährungsplattform Garantex

Bei operativen Maßnahmen gegen die russische Handels- und Kryptowährungsplattform Garantex beschlagnahmten die GenStA Frankfurt am Main / ZIT und das BKA zahlreiche Server sowie Kryptowährungen. Die Maßnahmen in einem Rechenzentrum in Karlsruhe erfolgten auf Ersuchen des United States Secret Service (USSS).

Garantex steht im Verdacht, als Geldwäschedienstleister für verschiedene kriminelle Gruppierungen unter anderem aus dem Phänomenbereich Cybercrime tätig gewesen zu sein. So sollen im Zeitraum von Januar 2019 bis November 2023 rund 1,18 Mio. Transaktionen mit einem Gesamtvolumen von rund 180.000 Bitcoin (zum damaligen Zeitpunkt umgerechnet etwa 14,4 Mrd. Euro) über Garantex abgewickelt worden sein. Ein bedeutender Teil der über Garantex gehandelten Werte kann auf kriminelle Aktivitäten, insbesondere Ransomware-Zahlungen, zurückgeführt werden. Im Februar hatte auch die Europäische Union in ihrem 16. Sanktionspaket gegen Russland die Sanktionierung der Plattform beschlossen. Zeitgleich zu den umfassenden Sicherstellungen in Deutschland stellten US-Behörden einen damaligen Gegenwert von rund 25 Mio. Euro in der Kryptowährung Tether sicher.

April: Darknet-Akteur Pygmalion und Kryptoplattform eXch

Maßnahmen gegen den Darknet-Akteur Pygmalion

Im Rahmen eines unter Sachleitung der GenStA Bamberg (ZCB) geführten Ermittlungsverfahrens gegen den Darknet-Akteur Pygmalion nahm das BKA zwei deutsche Beschuldigte fest und durchsuchte sechs Objekte in Niedersachsen, Nordrhein-Westfalen und Thüringen. Bei Pygmalion handelt es sich um einen Akteur, der zeitweise eigene Darknet-Plattformen betrieb und sowohl über das Darknet, als auch über verschiedene Messenger-Dienste bandenmäßig Betäubungsmittel in nicht geringer Menge vertrieb. Im Zuge der Maßnahmen wurden umfangreiche Beweismittel sowie Vermögenswerte sichergestellt. Im Anschluss an die Festnahmen und Durchsuchungen erfolgte die Sicherung des Servers, auf dem die Darknet-Plattform „Pygmalion Refuge“ betrieben wurde.

Maßnahmen gegen die Kryptoplattform eXch

Bei eXch handelte es sich um eine Plattform, die sowohl über das Clear- als auch das Darknet erreichbar war und über die Kryptowährungen in andere Währungen getauscht werden konnten. Die Betreiber warben aktiv damit, keine Geldwäschebekämpfungsmaßnahmen umzusetzen, also keine Nutzeridentifizierung (Know-Your-Customer/KYC) und kein Logging vorzunehmen. Über die Plattform wurde unter anderem ein Teil der 1,5 Mrd. US-Dollar gewaschen, die nordkoreanische Hacker von Bybit erbeutet haben[18].

Das BKA lokalisierte die Server-Infrastruktur hinter eXch in Deutschland. Um der täterseitig im April angekündigten Abschaltung der Plattform zum 01. Mai 2025 zuvorzukommen, wurden noch im selben Monat operative Maßnahmen durchgeführt. Dabei wurden die Festplatten des Servers entschlüsselt, der Dienst abgeschaltet und diverse Krypto-Wallets sowie eine Datenbank des Dienstes identifiziert. Damit war es möglich, Kryptowährungen mit einem Gesamtwert von zum damaligen Zeitpunkt ca. 34 Mio. Euro sicherzustellen.

18 Die Kryptobörse Bybit wurde im Februar 2025 Ziel eines Cyberangriffs. Mutmaßlich nordkoreanischen Cyberakteuren gelang es, in das System einzudringen und Ethereum (ETH) im Gegenwert von insgesamt 1,5 Mrd. US-Dollar von der Plattform zu entwenden. Bei Bybit handelt es sich um eine der größten Handelsplattformen des Kryptomarkts, auf der Vermögenswerte von ca. 60 Mio. Nutzerinnen und Nutzern verwaltet wird.

Mai: Operation Endgame 2.0

In einer international koordinierten Aktion nahmen die GenStA Frankfurt am Main / ZIT und das BKA gemeinsam mit Strafverfolgungsbehörden aus den Niederlanden, Frankreich, Dänemark, Großbritannien, Kanada und den USA sowie mit Unterstützung durch Europol und Eurojust die derzeit einflussreichsten Schadsoftware-Varianten vom Netz und identifizierten dahinterstehende Tatverdächtige. Die Maßnahmen richteten sich gegen die Dropper bzw. Loader Bumblebee, Latrodectus, Qakbot, DanaBot, HijackLoader, Warmcookie und Trickbot.

Die beteiligten Staaten entzogen den mutmaßlichen Tätern den Zugriff auf weltweit rund 300 Server, davon etwa 50 Server in Deutschland. Zudem konnten ca. 650 Domains unschädlich gemacht werden. Damit ist es den Strafverfolgungsbehörden gelungen, die technische Infrastruktur der Täter entscheidend zu schwächen. Zusätzlich wurden Kryptowährungen im Gesamtwert von damals umgerechnet 3,5 Mio. Euro sichergestellt und den Cyberkriminellen so eine erhebliche Menge ihrer finanziellen Basis entzogen.

In Deutschland wurden die Ermittlungen unter anderem wegen des Verdachts der banden- und gewerbsmäßigen Erpressung sowie der Mitgliedschaft in einer kriminellen Vereinigung im Ausland geführt. Auf dieser Grundlage konnten ZIT und BKA gemeinsam internationale Haftbefehle gegen 20 Akteure, weit überwiegend russische Staatsangehörige, erwirken und entsprechende Fahndungsmaßnahmen einleiten. Ergänzend haben die US-amerikanischen Behörden gegen 17 Akteure nach angloamerikanischem Recht Anklage erhoben (sogenannte „Indictments“).

Ziel der Operation Endgame ist es, die relevantesten Schadsoftware-Varianten der Kategorie „Initial Access Malware“ (sogenannte Dropper oder Loader) unschädlich zu machen. Schadsoftware dieser Kategorie wird zur Erstinfektion genutzt und dient Cyberkriminellen als Türöffner, um unbemerkt Opfersysteme zu infizieren und dann weitere Schadsoftware nachzuladen. Dies geschieht beispielsweise zum Ausspähen von Daten oder zur Verschlüsselung des Systems mit dem Ziel der Erpressung von Lösegeld (sogenannte Ransomware).

Juni: Operation Deep Sentinel

Unter Sachleitung der GenStA Frankfurt am Main/ZIT führte das BKA umfangreiche Exekutivmaßnahmen gegen den deutschen Administrator ASNT der Darknet Plattform „Archetyp Market“ durch. Bei dieser handelte es sich um eine der weltweit größten und am längsten bestehenden kriminellen Handelsplattformen im Darknet. Über den Marktplatz erfolgten ca. 2,3 Mio. abgeschlossene Bestellungen. Gehandelt wurden dort insbesondere Betäubungsmittel (unter anderem Amphetamin, Cannabis, Fentanyl, Heroin und Kokain) mit einem Gesamtumsatz in Höhe von mindestens 330 Mio. Euro.

Im Beisein von BKA-Kräften nahm die spanische Nationalpolizei den Beschuldigten in Barcelona fest. Bei diesem konnten Vermögenswerte in Höhe von ca. 9,5 Mio. Euro gesichert werden. Während der Actionweek sowie im Nachgang fanden 27 Durchsuchungsmaßnahmen in Deutschland, den Niederlanden, Rumänien, Schweden, Spanien, Thailand sowie den USA statt, bei denen es zu mehreren Festnahmen von Moderatoren und Vendoren von „Archetyp Market“ kam.

Juli: Operation Eastwood und Operation Checkmate

Operation Eastwood

Mitte Juli 2025 ging das BKA gemeinsam mit der GenStA Frankfurt am Main/ZIT sowie internationalen Partnerbehörden aus den USA, den Niederlanden, der Schweiz, Schweden, Frankreich, Spanien und Italien, unterstützt durch Europol und Eurojust sowie unter Beteiligung weiterer europäischer Länder, gegen Akteure und Infrastruktur der hacktivistischen Gruppierung NoName057(16) vor.

Den Strafverfolgungsbehörden gelang es, ein aus mehreren hundert weltweit verteilten Servern bestehendes Botnetz abzuschalten, das die Täterschaft für gezielte DDoS-Angriffe einsetzte. In Deutschland wurden sechs Haftbefehle gegen russische Staatsangehörige bzw. in der Russischen Föderation wohnhafte Beschuldigte erwirkt. Zwei dieser Personen wird vorgeworfen, die Rädelsführer von NoName057(16) zu sein. Darüber hinaus wurde ein weiterer Haftbefehl durch die spanischen Behörden erlassen.

Nach allen Beschuldigten wird international gefahndet. Außerdem wurden Durchsuchungsmaßnahmen an insgesamt 24 Objekten von mutmaßlichen Unterstützern der Gruppierung durchgeführt, darunter in Berlin und Bayern.

Ergänzend wurden mehr als 1.000 Unterstützerinnen und Unterstützer der hacktivistischen Gruppierung mittels des täterseitig genutzten Messengerdienstes Telegram über die behördlichen Maßnahmen informiert und auf die Strafbarkeit der Handlungen nach deutschem Recht aufmerksam gemacht. In Deutschland wird durch ZIT und BKA gegen die Rädelsführer, Mitglieder sowie Unterstützerinnen und Unterstützer der Gruppierung unter anderem wegen des Verdachts der Bildung einer kriminellen Vereinigung im Ausland zum Zwecke der Computersabotage ermittelt.

Operation Checkmate (LKA Niedersachsen)

Seit 2022 werden im LKA Niedersachsen die Zentralen Ermittlungen zu der Ransomware Royal/BlackSuit in der Operation Checkmate geführt. Die Ransomware Royal (ab Mai 2023 Rebranding zu BlackSuit) ist ein internationaler Zusammenschluss aus Cyberkriminellen, die ihren Ursprung vermutlich in der mittlerweile aufgelösten Ransomware-Gruppierung Conti haben. Im Gegensatz zu vielen anderen Gruppierungen arbeitet BlackSuit nicht als Ransomware-as-a-Service mit vielen Partnern (Affiliates) zusammen, sondern operiert als geschlossene, professionelle Kerngruppe und nutzt den Modus Operandi Double Extortion. Weltweit wird von 550 bis 600 Geschädigten ausgegangen. Der geschätzte Gesamtschaden liegt bei ca. 500 Mio. US-Dollar. Innerhalb der Operation Checkmate werden 29 Royal- und zehn BlackSuit-Fälle in Deutschland geführt. Der hierbei durch Lösegeldzahlungen entstandene Schaden liegt bei ca. 1,5 Mio. Euro. Im Rahmen der Ermittlungen ist es dem LKA Niedersachsen in enger Zusammenarbeit mit dem BKA und dem US-amerikanischen Department of Homeland Security gelungen, die Darknet-Infrastruktur der Täter aufzuklären. In einer mithilfe von Europol koordinierten Aktion übernahm das LKA zusammen mit den international beteiligten Partnern die Infrastruktur der Tätergruppierung. Die hierbei gewonnen Informationen haben außerdem zu der Identifizierung mehrerer nichtdeutscher Tatverdächtiger geführt.

November: Operation Endgame 3.0 und Takedown des Bitcoin-Mixers cryptomixer.io

Operation Endgame 3.0

Im Fokus der Operation Endgame 3.0 standen einer der gefährlichsten Stealer sowie einer der meistgenutzten Fernzugriffs-Trojaner (Remote Access Trojan, kurz: RAT) weltweit. Die GenStA Frankfurt am Main / ZIT und das BKA machten diese in einer international abgestimmten Aktion gemeinsam mit Strafverfolgungsbehörden aus den Niederlanden, Frankreich, Dänemark, Belgien und den USA sowie mit Unterstützung durch Australien, Kanada, das Vereinigte Königreich, Europol und Eurojust unschädlich.

In Folge der internationalen Ermittlungen als Teil der Operation Endgame schalteten die Strafverfolgungsbehörden die technische Infrastruktur von Rhadamanthys, einem der gefährlichsten Stealer[19] weltweit, ab. Die Maßnahmen richteten sich gegen mehr als 1.000-täterseitig genutzte Server, davon über 180 in Deutschland. In diesem Zusammenhang wurden kompromittierte Opferdaten im hohen zweistelligen Millionenbereich von über 650.000 Opfern sichergestellt und über Informationsplattformen der Öffentlichkeit zum individuellen Abgleich bereitgestellt. Darüber hinaus wurden erfolgreich Maßnahmen gegen eine der wichtigsten Remote Access Trojan-Varianten, VenomRAT, umgesetzt.

Im Zuge der internationalen Ermittlungen ist eine Festnahme in Griechenland sowie die Durchsuchung von elf Objekten, darunter eines in Deutschland, erfolgt.

Darüber hinaus haben die Strafverfolgungsbehörden Kryptowerte in Höhe von über 200 Mio. US-Dollar von führenden Kryptowährungsbörsen sperren lassen. Die Möglichkeiten der Cyberkriminellen, Kryptowährung in andere Währungen umzutauschen, wurden dadurch erheblich eingeschränkt.

In Deutschland wurden die Ermittlungen insbesondere wegen des Verdachts der Erpressung im besonders schweren Fall geführt.

19 Stealer zielen darauf ab, unbemerkt sensible Daten von infizierten Systemen zu stehlen. Nach der Infektion durchsuchen sie das infizierte System automatisiert nach sensiblen Informationen und leiten diese aus.

Takedown cryptomixer.io

Die Stadtpolizei Zürich übernahm die in der Schweiz befindliche Infrastruktur des Bitcoin-Mixers cryptomixer.io. Dabei konnten Kryptowerte in einer Gesamthöhe von ca. 25 Mio. Euro sichergestellt werden. Vorausgegangen waren gemeinsame Ermittlungen zwischen der Stadtpolizei, der Kantonspolizei Zürich sowie dem BKA. Das Ermittlungsverfahren wurde von Europol und Eurojust unterstützt.

Der Mixing-Dienst Cryptomixer.io ermöglichte Kunden, Transaktionen auf der Bitcoin-Blockchain zu verschleiern, um somit vor allem die Rückverfolgung der Vermögenswerte für Strafverfolgungsbehörden massiv zu erschweren. Der Dienst war bereits seit März 2016 aktiv und verarbeitete seither Vermögenswerte in Milliardenhöhe. Ein Großteil der Vermögenswerte stammte dabei aus Darknet-Marktplätzen, Ransomware-Angriffen und Betrugsfällen.

5 Quo Vadis, Cybercrime?

Im Jahr 2025 bestätigen sich die Trends der Vorjahre: Eine Zunahme aller relevanten Fallzahlen für Ransomware, DDoS und Hacktivismus resultiert in einer sich weiter zuspitzenden Bedrohungslage im Phänomenbereich Cybercrime. Darüber hinaus führen die weiter fortschreitenden Entwicklungen im Bereich der KI zu einer erhöhten Skalierbarkeit bestehender Angriffsmuster, verbunden mit einer Steigerung der Angriffsqualität.

Auf Basis der im vergangenen Jahr erhobenen Kennzahlen ist auch im Jahr 2026 mit einer quantitativen und qualitativen Steigerung der Bedrohungslage zu rechnen. Relevante Einflussfaktoren für eine wachsende Anzahl an Cyberangriffen sind neben den steigenden technischen Fähigkeiten der cyberkriminellen Akteure die Weiterentwicklung von KI-Tools und deren missbräuchliche Nutzung. Auch die Nutzung von Quantencomputing wird perspektivisch die Cyberkriminalität beeinflussen, da hierdurch beispielsweise sensible Daten schneller entschlüsselt werden können. Zudem ist weiterhin mit einer schnellen Anpassungsfähigkeit von Cyberkriminellen zu rechnen, was sich bereits 2025 unter anderem im Bereich Ransomware beim Wechsel des Modus Operandi hin zu einer verstärkten Nutzung von Data Extortion zeigte.

Auch zukünftig ist mit einer Intensivierung der Bedrohungslage zu rechnen.

Um dieser erhöhten Bedrohungslage im Cyberraum effektiv zu begegnen, setzt das BKA auf einen Vier-Ebenen-Ansatz mit dem Ziel, die teilweise hochprofessionellen Cybergruppierungen zu zerschlagen. Die Bekämpfungsstrategie basiert auf einem personenbezogenen Ansatz, der Zerschlagung technischer Infrastrukturen, dem Entzug finanzieller Mittel sowie einer disruptiven Kommunikation mit dem Ziel von Reputationsschäden in der cyberkriminellen Szene. Ein herausragender Erfolg dieses Ansatzes spiegelt sich hierbei unter anderem in der vom BKA koordinierten Operation Endgame wider, bei der wesentliche Malware-Familien, die zur Erstinfektion von IT-Systemen genutzt werden, im Fokus polizeilicher Maßnahmen stehen und hierdurch nachweislich an Relevanz für die kriminelle Szene verloren haben.

Der mehrdimensionale Ermittlungsansatz bewirkt eine nachhaltige Strafverfolgung.

Geopolitische Konflikte, die sich spätestens seit dem Jahr 2022 zunehmend auch in den Cyberraum verlagern und zu einer Mobilisierung hacktivistischer Gruppierungen führen, bleiben ein kritischer Faktor mit hohem Eskalationspotenzial. Als führendes Mitglied der Europäischen Union und der NATO steht Deutschland im Fokus von vor allem politisch motivierten Cyberangriffen. Auch staatliche Akteure nutzen verschiedene Methoden, um deutsche Ziele anzugreifen. Viele Staaten unterhalten professionell aufgestellte und ausgestattete Cyberabteilungen bei ihren Nachrichtendiensten oder Streitkräften, die unter anderem kritische Infrastrukturen, Behörden und relevante Ziele anderer Länder ausspionieren oder sabotieren. Dies verschärft die Bedrohungslage angesichts laufender Krisen und Kriege weiter. Um auch auf diesen Aspekt angemessen zu reagieren und bewährte Strategien aus der Bekämpfung der finanziell motivierten Cybercrime auf den Bereich der staatlich gesteuerten Cybercrime auszuweiten, wurden im BKA die Ermittlungskapazitäten beider Bereiche organisatorisch gebündelt. Der weitere Ausbau der Fähigkeiten vor allem mit Blick auf die im Phänomenbereich stark technisch geprägten Ermittlungen stellt einen wesentlichen Beitrag zur Gewährleistung der Cybersicherheit in Deutschland dar.

Ausschlaggebend für die zukünftige Entwicklung der Bedrohungslage im Cyberraum wird angesichts der aktuellen geopolitischen Lage insbesondere die Reaktionsfähigkeit Deutschlands auf laufende oder bevorstehende Cyberangriffe sein. Solche Angriffe realisieren sich in vielen Fällen nicht örtlich begrenzt, sondern länderübergreifend oder gar bundesweit, weshalb insbesondere bei schwerwiegenden Cyberangriffen eine internationale Koordination und Reaktionsmöglichkeit auf Bundesebene erforderlich ist.

Die stetig steigende Bedrohungslage erfordert eine erhöhte Reaktionsfähigkeit der Strafverfolgungsbehörden.

Anders als in Fällen des internationalen Terrorismus besteht für das BKA bisher allerdings keine Möglichkeit zur Abwehr solcher Gefahren im Phänomenbereich Cybercrime. Um diese Lücke zu schließen, soll dem BKA – anknüpfend an seine bestehende Zuständigkeit für die internationale polizeiliche Zusammenarbeit – in einem laufenden Gesetzgebungsverfahren eine Aufgabe zur polizeilichen Gefahrenabwehr im Cyberraum zugewiesen werden (Cyberabwehr).

Die Bündelung von Kompetenzen der Strafverfolgung und der Gefahrenabwehr ist für die nationale Sicherheit Deutschlands im Cyberraum zwingend erforderlich.

Der Fokus liegt hierbei insbesondere auf der Abwehr schwerwiegender und länderübergreifender Cyberangriffe, die angesichts der bestehenden Dynamik von Cybercrime bisher nicht oder nicht zeitgerecht adressiert werden können. Das BKA verfügt über die notwendigen technischen Fähigkeiten und Kompetenzen sowie nationale und internationale Netzwerke, um diese Aufgabe umzusetzen. Die Verbindung von Strafverfolgung und Gefahrenabwehr ermöglicht hierbei künftig eine effektive Reaktion auf die bestehende Bedrohungslage im Phänomenbereich Cybercrime.

Bundeslagebild Cybercrime 2025

Impressum

Herausgeber
Bundeskriminalamt, 65173 Wiesbaden

Redaktion
Bundeskriminalamt, 65173 Wiesbaden

Stand
Mai 2026

Gestaltung
Bundeskriminalamt, 65173 Wiesbaden

Bildnachweis
Bundeskriminalamt

Weitere Lagebilder des Bundeskriminalamtes
zum Herunterladen finden Sie ebenfalls unter:
www.bka.de/Lagebilder

Whatsapp-Kanal

www.bka.de

facebook.com/bundeskriminalamt.bka
linkedin.com/company/bundeskriminalamt
instagram.com/Bundeskriminalamt
youtube.com/BundeskriminalamtBKA