HOCHSCHULE MITTWEIDA
University of Applied Sciences

Fraunhofer SIT

Bundeskriminalamt

Rechtsgrundlagen II
Prüfungsschwerpunkte

Prof. Dr. rer. nat. Dirk Labudde

Definitionen Cybercrime

Was ist Cybercrime?

Cybercrime umfasst die Straftaten, die sich gegen das Internet, Datennetze, informationstechnische Systeme oder deren Daten richten (Cybercrime im engeren Sinne) oder die mittels Informationstechnik begangen werden (Cybercrime im weiteren Sinne).

Definitionen Cybercrime

Unter Cybercrime oder IuK-Kriminalität werden Straftaten verstanden, die unter Ausnutzung moderner Informations- und Kommunikationstechnik gegen diese begangen werden. Dazu zählen:

- alle Straftaten, bei denen Elemente der EDV in den Tatbestandsmerkmalen enthalten sind (Computerkriminalität) oder bei denen die IuK zur Planung, Vorbereitung oder Ausführung einer Tat eingesetzt wird/wurde
- Straftaten im Zusammenhang mit Datennetzen wie z.B. dem Internet
- Fälle der Bedrohung von Informationstechnik

Letzteres schließt alle widerrechtlichen Handlungen gegen die Integrität, Verfügbarkeit und Authentizität von elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeicherten oder übermittelten Daten (Hacking, Computersabotage, Datenveränderung, Missbrauch von Telekommunikationsmitteln etc.) ein.

Definitionen Cybercrime

Bei der Computerkriminalität im engeren Sinn handelt es sich um Delikte, bei denen in den Tatbestandsmerkmalen der jeweiligen Norm (Straftat oder auch Ordnungswidrigkeit) Elemente der elektronischen Datenverarbeitung genannt sind. Darunter fallen beispielsweise der Computerbetrug (§ 263a StGB), das Ausspähen und Abfangen von Daten (§§ 202a, 202b, 202c StGB), die Datenveränderung sowie die Datensabotage (§§ 303a und 303b StGB), Fälschung beweiserheblicher Daten (§ 269 StGB) oder die Störung öffentlicher Betriebe (§ 316b StGB). Daneben befassen sich weitere Gesetze mit diesen Deliktarten. So zum Beispiel das Urheberrechtsgesetz (UrhG), das Bundesdatenschutzgesetz (BDSG), das Telekommunikationsgesetz (TKG), das Gesetz gegen den 8 unlauteren Wettbewerb (UWG) oder das Gesetz über den Schutz von Marken und sonstigen Kennzeichen (MarkenG).

Definitionen Cybercrime

Unter den Begriff Computerkriminalität im weiteren Sinn fallen Straftaten, für deren Durchführung ein elektronisches Datenverarbeitungssystem unter Einbezug von Informations- und Kommunikationstechnik genutzt wird. Dazu zählen zum Beispiel der Warenkreditbetrug, Propagandastraftaten aus extremistischen Kreisen, Gewaltverherrlichung, das Verbreiten von Kinderpornografie oder Beleidigungstatbestände.

Mit der weltweiten Zunahme der Internetnutzung wird die Verbreitung strafbarer Inhalte dieser Kategorien vereinfacht.

Definitionen Cybercrime

Aus der Definition lassen sich insofern Tathandlungen ableiten, zu deren Begehung das Internet und vorhandene gespeicherte Daten genutzt (Phishing, Betrug, Urheberrechtsverletzungen, Kreditkartenmissbrauch oder Propagandastraftaten, Cybermobbing), neue Daten generiert und veröffentlicht (Verbreitung von (Kinder-)Pornographie, Verbreitung terroristischer Ideologien, Gewaltdarstellungen, Aufstachelung zum Rassenhass) oder Angriffe auf das Medium Internet selbst durchgeführt werden (Verbreitung von Viren, Würmern und Trojanern, Eindringen in PC-Anlagen zur Datenänderung, Datenlöschung oder zum Datendiebstahl, „Denial of Service“ -Attacken).

Zusammenfassung

Es gibt keine einheitliche Beschreibung, bzw. Definition von Cybercrime.

Aktuell drei Arten der Differenzierung:

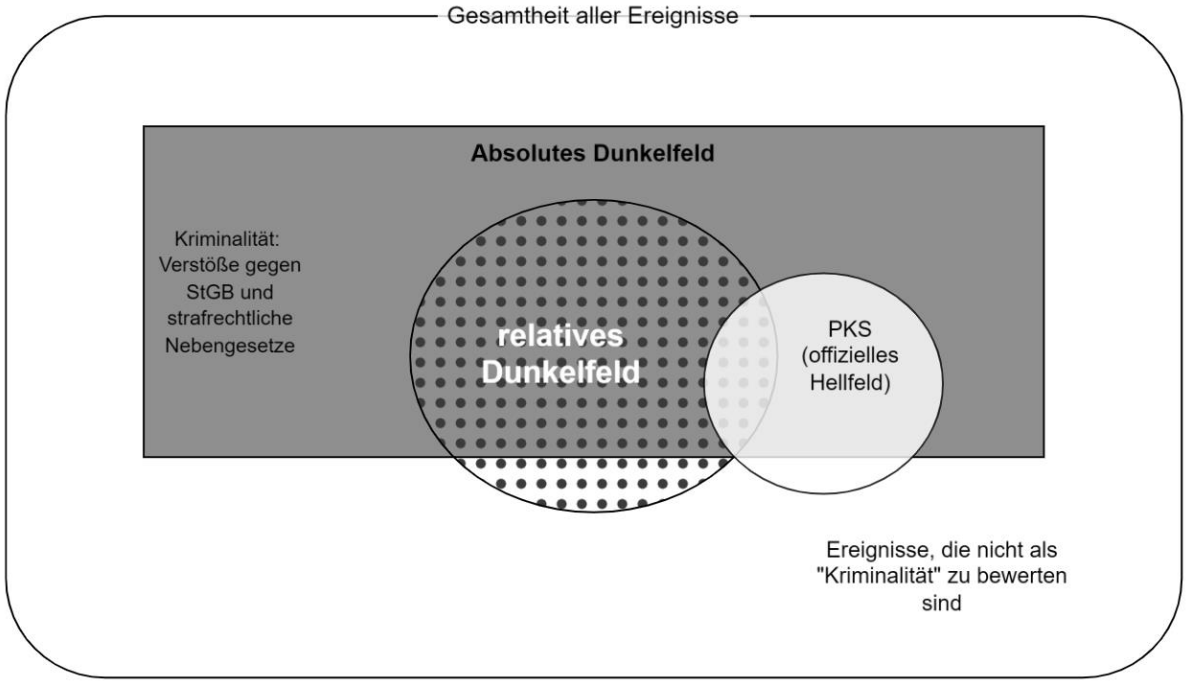
Variante 1: Cybercrime im engeren Sinn (Core Cybercrime bzw. Cyberdependent Crime): alle Delikte, die es in keiner Variante offline gibt

Variante 2: Cybercrime im weiteren Sinn (Non-cyberspecific Cybercrime bzw. Cyberenabled Crime): Delikte, die unter diese Kategorie fallen, können auch offline existieren Variante

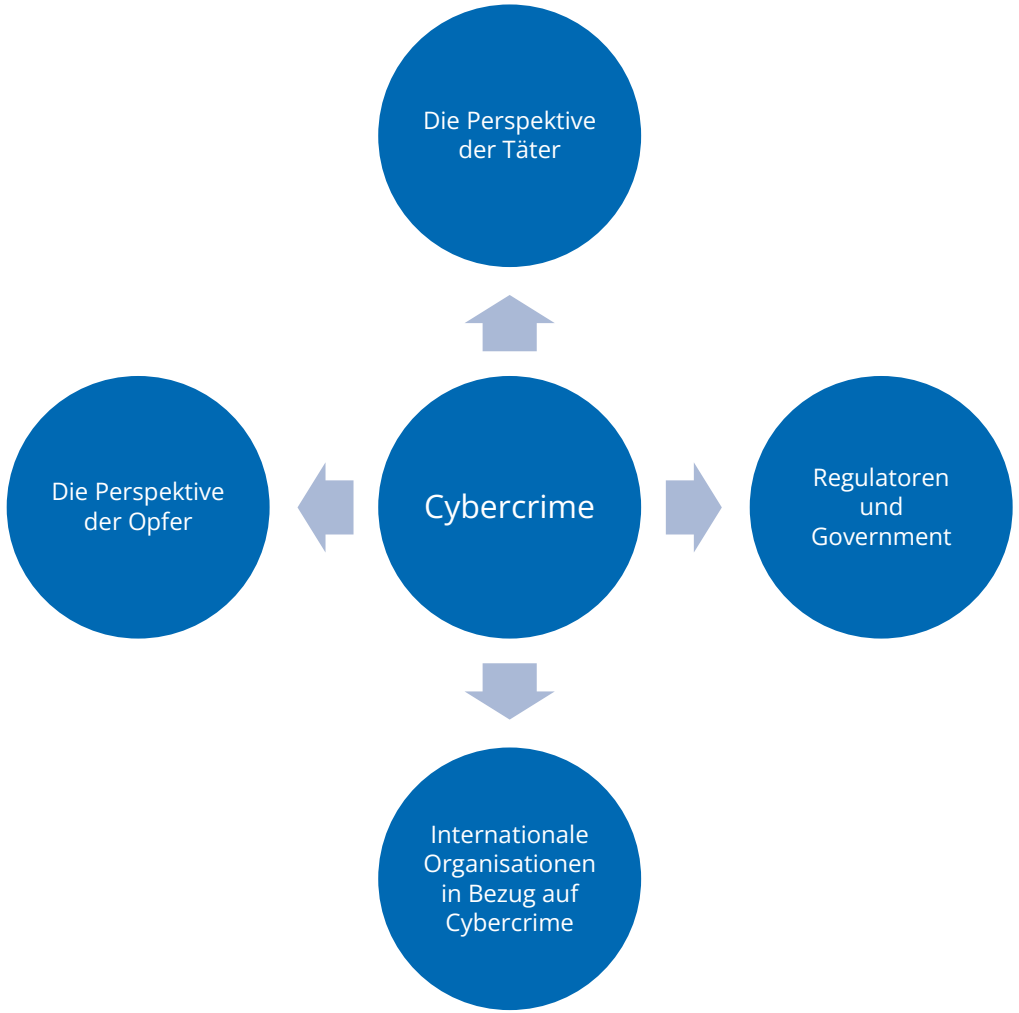
3: Verschleierung der Identität: Dies betrifft Täter, die sich einen Online-Avatar zulegen und die Anonymität dazu verwenden, kriminell zu handeln, bzw. Täter, die sich gestohlener Identitäten oder Fake-Identities bedienen.

Hellfeld vs. Dunkelfeld

- Hellfeld: Summe aller Straftaten (Kriminalität), die den Strafverfolgungsbehörden bekannt ist, also offiziell registrierte Straftaten
- Absolutes Dunkelfeld: Summe aller Straftaten (Kriminalität), die den Strafverfolgungsbehörden nicht bekannt ist
- Relatives Dunkelfeld: schließt offiziell nicht erfasste, aber durch Befragungen bekannte Straftaten mit ein



Relevante Akteure



Europol

Zum Thema Cybercrime definiert Europol folgendes:

- Die Intensität von Cybercrime hängt von kulturellen, juristischen, wirtschaftlichen und regionalen Einflussfaktoren ab;
- traditionelle Methoden der Verbrechensbekämpfung greifen hier nicht mehr. Elektronische ‚Beweise' verteilen sich oft über mehrere Orte der Welt, was ein Auffinden der Täter erschwert;
- in einer Welt von Cloud Computing muss sich die Legislative künftig überlegen, welche Beweise zur Verurteilung von Tätern in Frage kommen, damit eine effiziente Strafverfolgung möglich wird;
- es bedarf einer Harmonisierung der nationalen Rechte, um eine Strafverfolgung im internationalen Umfeld zu erleichtern und
- die Cybercrime-Prävention muss in allen Ländern im Vordergrund stehen

Cyberkriminologie

Neue Formen von sozialer Abweichung, von Straftaten, von Opferwerdungen aber auch von sozialer und staatlicher Kontrolle entstehen und erfordern einen radikal neuen Ansatz der Kriminologie: Die Cyberkriminologie erforscht:

- Ursachen
- Zusammenhänge
- Präventionsmöglichkeiten von Straftaten

die im virtuellen Raum geschehen und Auswirkungen auf die physische Realität haben.

Strafprozessordnung (StPO)

- Rechtsnorm in Deutschland, regelt das Strafverfahren vor deutschen Gerichten
- Bestimmt Verfahrensabläufe, Rechte und Pflichten von Staatsanwaltschaft, Gericht, Verteidigung und Angeklagten
- Enthält Regelungen zur Beweisaufnahme, zum Verfahrensablauf, zur Verhandlungsführung und zu Rechtsmitteln
- Gewährleistet fairen und rechtsstaatlichen Ablauf von Strafverfahren

→ § 100a Telekommunikationsüberwachung

Telekommunikationsüberwachung (TKÜ)

- Gesetzlich verankert in § 100a Abs. 1 S. 2, 3 StPO und für das BKA zur Terrorismusbekämpfung nach §§ 5, 51 Abs.2 BKAG
- Maßnahme zur Überwachung von Telekommunikation, um strafrechtlich relevante Informationen zu sammeln
- Ermöglicht staatlichen Behörden wie Polizei oder Geheimdiensten die Überwachung von Telefonaten, E-Mails, SMS, Internetnutzung usw.
- Dient der Bekämpfung von schweren Straftaten wie Terrorismus, Organisierter Kriminalität, Drogenhandel usw.
- Erfordert richterliche Genehmigung und Einhaltung strenger rechtlicher Vorgaben zum Schutz der Privatsphäre und Grundrechte

Kriminalstatistiken in Deutschland

Kriminalstatistik

- Amtliche kriminologische Statistiken, die strafbares und rechtswidriges Verhalten quantitativ erfassen
- Sind regional begrenzt auf wohldefinierte Gebiete, wie z.B. Staatsgebiete oder Bundesländer
- Geben Aufschluss über:
  - Täter und deren Gruppierungen
  - Opfer
  - Fälle
  - Ermittlungsverfahren
  - Schäden
  - Strafrechtliche Folgen

PKS – wichtige Zahlen

- Erfasste Straftaten:
  - Straftaten und unter Strafe gestellte Versuche gelten nur dann als erfasster Fall, wenn sie der Polizei auf irgendeinem Wege bekannt geworden sind
  - Durch Anzeige eines Bürgers, Entdeckung einer Straftat durch die Polizei, anderweitig Kenntnis erlangt

- Aufklärungsquote (AQ):
  - Anzahl der aufgeklärten Straftaten als Anteil der insgesamt erfassten Straftaten
  - Berechnung:

$$AQ = \frac{auf gklärte\ Fälle \cdot 100}{bekannt\ gewordene\ Fälle}$$

PKS – abschließende Frage

Ist die PKS gut geeignet, um Cybercrime vollumfänglich darzustellen?

- NEIN!
- Die PKS hat im Rahmen von Cybercrime folgende Probleme:
  - Einmalerfassung der Fälle
  - Schadensmeldungen (Sachschaden, Ausfallzeit)
  - Auslandsbezug
  - Tatort unbekannt
  - Tateinheiten (z.B. Ransomware)
  - Geänderte Schlüssel
  - Keine Ausreichende Analyse der Opfer

Bundeslagebild Cybercrime

Lagebild

- Sammlung von georeferenzierten echtzeitnahen Daten
- Informationen von Behörden, Sensoren und Plattformen, die über gesicherte Kanäle übermittelt wurden
- Ziel: Teilen der zusammengetragenen Informationen mit anderen informationsbedürftigen Einheiten, um ein Lagebewusstsein zu erlangen und Reaktionsfähigkeit zu verbessern

Bundeslagebild Cybercrime

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 die diesbezüglichen Ergebnisse polizeilicher Strafverfolgungsaktivitäten ab.

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

Delikte, die lediglich unter Nutzung von Informationstechnik begangen werden und bei denen das Internet vorwiegend Tatmittel ist (sogenannte Cybercrime im weiteren Sinne, CCiwS), werden nicht der CCieS zugeordnet und bleiben bei den Betrachtungen im Bundeslagebild Cybercrime weitestgehend unberücksichtigt.

Cybercrime im engeren Sinne

Rückgang der erfassten Cyberstraftaten um 6,5% (Inlands-PKS). Auslandstaten steigen an.

Die Aufklärungsquote für Cybercrime bewegt sich mit ca. 29% auf dem Niveau des Vorjahres.

Der russische Angriffskrieg auf die Ukraine birgt auch im Cyberraum massives Eskalationspotential.

Ransomware bleibt primäre Bedrohung für Unternehmen und öffentliche Einrichtungen.

Phishing ist Haupteintrittsvektor für Schadsoftware und passt sich aktuellen gesellschaftlich relevanten Themen an.

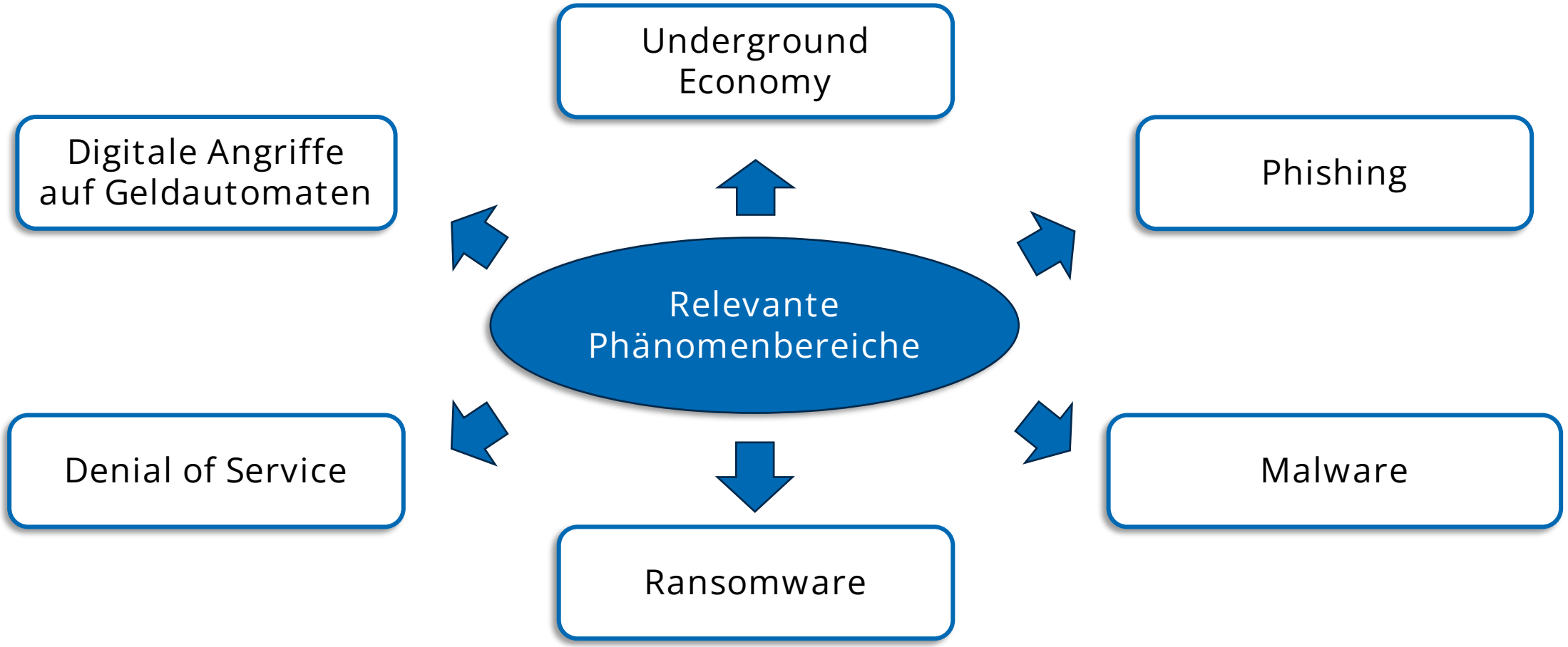
DDoS-Angriffe werden effizienter.

Zum Jahresende 2022 erfolgten vermehrt Angriffe auf das Bildungswesen.

Die vom Bitkom e.V. bezifferten Schäden u.a. durch Cyberangriffe belaufen sich auf 202,7 Mrd. Euro.

Weniger Unternehmen gehen auf Erpressungsforderungen von Cybertätern ein.

Cybercrime im engeren Sinn



Zusammenfassung

- Alle der Polizei bekannt gewordenen Straftaten werden durch die Polizeiliche Kriminalstatistik erfasst
- Cybercrime im engeren Sinne wird außerdem durch das Bundeslagebild Cybercrime abgebildet
- Die PKS ist aufgrund mehreren Faktoren nicht für die vollumfängliche Darstellung des Ausmaßes von CCies geeignet
- Cybercrime im weiteren Sinne kann nur bedingt analysiert werden mittels der PKS
  - Grundtabelle T05 – Straftaten mit Tatmittel Internet
  - Modus Operandi und anderen Metainformationen zu den Taten müssen aus anderen Quellen bezogen werden.

Das Netzwerkdurchsetzungsgesetz

Bundesministerium der Justiz

Regeln gegen Hass im Netz – das Netzwerkdurchsetzungsgesetz

Das Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz – NetzDG) ist seit dem 1. Oktober 2017 in Kraft.

Das Gesetz zielt darauf, **Hasskriminalität, strafbare Falschnachrichten und andere strafbare Inhalte auf den Plattformen sozialer Netzwerke wirksamer zu bekämpfen**. Dazu zählen z.B. Beleidigung, üble Nachrede, Verleumdung, öffentliche Aufforderung zu Straftaten, Volksverhetzung, Gewaltdarstellung und Bedrohung. Um die sozialen Netzwerke zu einer zügigeren und umfassenderen Bearbeitung von Beschwerden insbesondere von Nutzerinnen und Nutzer über Hasskriminalität und andere strafbare Inhalte anzuhalten, wurden mit dem NetzDG gesetzliche Compliance-Regeln für soziale Netzwerke eingeführt.

Dies beinhaltet eine gesetzliche Berichtspflicht für Anbieterinnen und Anbieter sozialer Netzwerke über den Umgang mit Hasskriminalität und anderen strafbaren Inhalten, Vorgaben zum Vorhalten eines wirksamen Beschwerdemanagements sowie zur Benennung eines inländischen Zustellungsbevollmächtigten. Verstöße gegen diese Pflichten können mit Bußgeldern gegen das Unternehmen und die Aufsichtspflichtigen geahndet werden. Außerdem wird Opfern von Persönlichkeitsrechtsverletzungen im Netz ermöglicht, aufgrund gerichtlicher Anordnung die Bestandsdaten der Verletzerinnen und Verletzer von den Diensteanbietendenrn zu erhalten.

https://www.bmj.de/DE/Themen/FokusThemen/NetzDG/NetzDG_node.html

https://www.bmj.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/RegE_Aenderung_NetzDG.pdf?__blob=publicationFile&v=2

Grundlagen für die Verfolgung von Cybercrime-Delikten

Gesetzesgrundlagen

Mit dem Inkrafttreten der Cybercrime Konvention in Deutschland am 01.07.2009 wurde das deutsche Strafrecht an die aktuellen Entwicklungen im Bereich der Internet- und Computerstraftaten angepasst.

Allerdings werden in dieser Konvention **keine Straftatbestände** festgelegt, sondern **Kategorien** gebildet, denen jeder Mitgliedstaat seine strafbewehrten Handlungen zuordnen kann oder in Ermangelung entsprechender Tatbestände verpflichtet ist, neue Gesetze zu erlassen.

Nationale Umsetzung

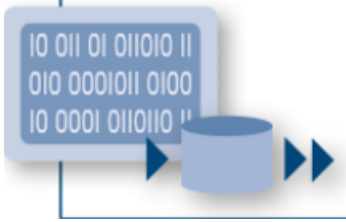
Vergleich beider Statistiken

Polizeiliche Kriminalstatistik	Bundeslagebild Cybercrime
Jährliche Zusammenstellung registrierter Kriminalität in Deutschland	Spezialisierte Analyse der Cyberkriminalität in Deutschland und im internationalen Raum
Basiert auf den Daten der Landeskriminalämter	Basiert auf der PKS + Anreicherung durch externe Erkenntnisse und Expertise
Darstellung aller Kriminalitätsbereiche	Konzentration auf Cybercrime im engeren Sinne
Ziel: ➢ Trends aufzeigen ➢ Arbeit der Polizei zu bewerten ➢ Kriminalpolizeiliche Maßnahmen planen	Ziel: ➢ Analyse der Täterverhalten ➢ Identifikation der Täterstrukturen ➢ Bedrohungs- und Risikobewertung ➢ Definition von Präventionsmaßnahmen

Grundlagen für die Verfolgung von Cybercrime-Delikten – Paragrafen

Straftatbestände	Inhalt (Kurzbeschreibung)
§202a StGB Ausspähen von Daten 	Das unbefugte Verschaffen eines Zugangs zu Daten, die nicht für den Täter bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung.
§ 202b StGB Abfangen von Daten 	Das unbefugte Verschaffen von Daten aus einer nichtöffentlichen Datenübermittlung oder aus der elektromagnetischen Abstrahlung einer Datenverarbeitungsanlage unter Anwendung von technischen Mitteln.

Grundlagen für die Verfolgung von Cybercrime-Delikten – Paragraphen

§ 202c StGB Vorbereiten des Ausspähens und Abfangens von Daten 	Das Vorbereiten einer o. g. Straftat durch das Herstellen, Verschaffen, Verkaufen, Überlassen, Verbreiten oder Zugänglichmachen von Passwörtern, Sicherheitscodes oder Computerprogrammen, deren Zweck die Begehung einer solchen Tat ist.
§ 202d StGB Datenhehlerei 	Das sich oder einem anderen Verschaffen, Überlassen, Verbreiten oder Zugänglichmachen von nicht allgemein zugänglichen und durch einen anderen aus einer rechtswidrigen Tat erlangten Daten mit der Absicht, sich oder einen Dritten zu bereichern oder einen anderen zu schädigen.

Grundlagen für die Verfolgung von Cybercrime-Delikten – Paragraphen

§263a StGB Computer-betrug

Das Schädigen des Vermögens eines Anderen durch Beeinflussung des Ergebnisses eines Datenverarbeitungsvorgangs durch unrichtige Gestaltung des Programms, durch Verwendung unrichtiger oder unvollständiger Daten, durch unbefugte Verwendung von Daten oder sonst durch unbefugte Einwirkung auf den Ablauf.

Des Weiteren das Vorbereiten einer solchen Tat durch Herstellung, Verschaffung, Feilhalten, Verwahren oder Überlassung eines Computerprogramms, deren Zweck die Begehung einer solchen Tat ist.

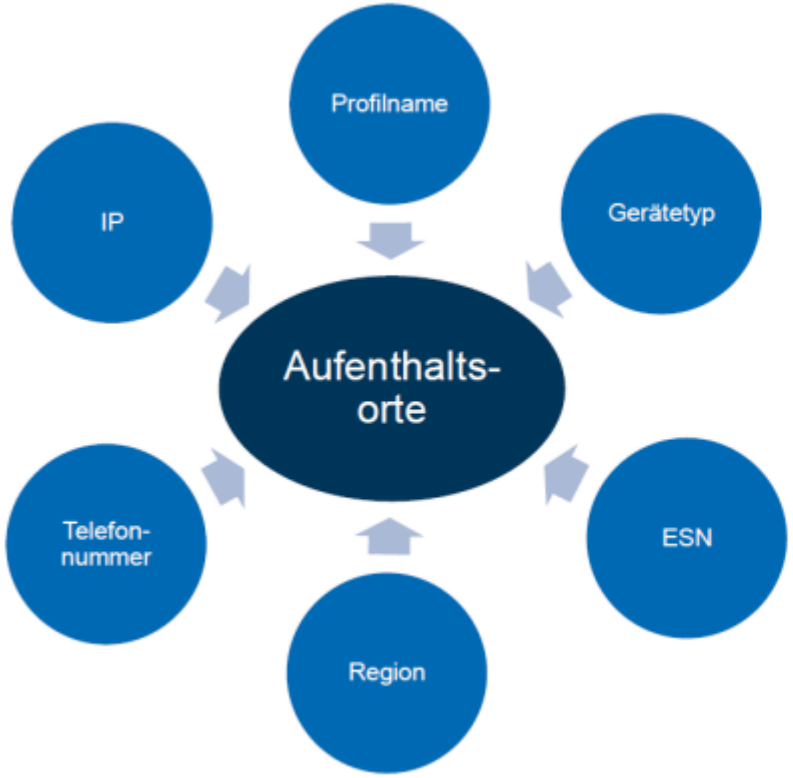
Grundlagen für die Verfolgung von Cybercrime-Delikten – Paragraphen

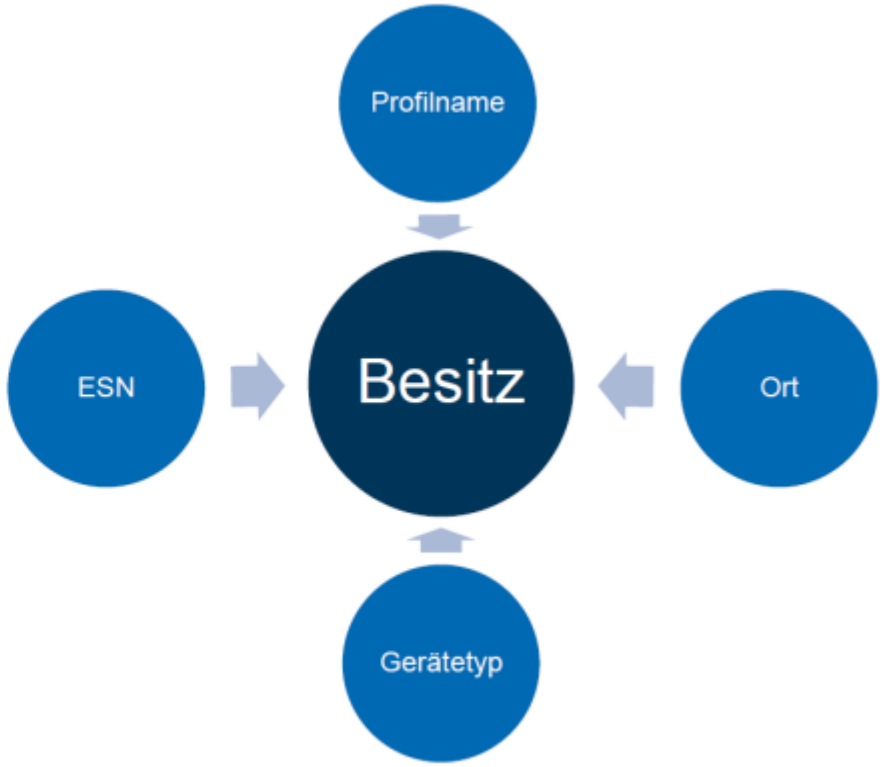
Das Speichern oder Verändern beweiserheblicher Daten zur Täuschung im Rechtsverkehr, so dass bei ihrer Wahrnehmung eine unechte oder verfälschte Urkunde vorliegen würde, oder das Gebrauchen solcher Daten.	**§269 StGB Fälschung beweiserheblicher Daten**
Das rechtswidrige Löschen, Unterdrücken, Unbrauchbarmachen oder Verändern von Daten.	**§303a StGB Datenveränderung**

Grundlagen für die Verfolgung von Cybercrime-Delikten – Paragraphen

Das erhebliche Stören einer Datenverarbeitung, die für einen anderen von wesentlicher Bedeutung ist, durch 1. Begehung einer Datenveränderung (§ 303a), 2. Eingabe oder Übermittlung von Daten in der Absicht, einem anderen Nachteil zuzufügen, oder 3. Zerstörung, Beschädigung, Unbrauchbarmachen, Beseitigen oder Verändern einer Datenverarbeitungsanlage oder eines Datenträgers.	**§303b StGB Computersabotage**

Profiling und Identität





Profiling und Identität

Identitätsdiebstahl

- Die illegale Erfassung und Nutzung persönlicher Identifikationsdaten einer Person durch eine andere Partei
- Beinhaltet das Sammeln sensibler Informationen wie Namen, Geburtsdaten, Sozialversicherungsnummern, Kreditkarteninformationen usw.
- Kann durch verschiedene Methoden erfolgen, darunter Phishing, Malware, Social Engineering oder den Diebstahl physischer Dokumente
- Zweck ist oft finanzieller Betrug, Identitätsmissbrauch oder Zugriff auf vertrauliche Informationen
- Kann zu schwerwiegenden finanziellen Verlusten, rechtlichen Problemen und persönlichen Belastungen für das Opfer führen
- Erfordert oft umfangreiche Maßnahmen zur Wiederherstellung der Identität und zur Absicherung persönlicher Informationen

Cybermobbing, Cyberbullying

Unter Cyberbullying oder Cybermobbing versteht man die Beleidigung, Bedrohung, Bloßstellung oder Belästigung von Personen mithilfe von Kommunikationsmedien, beispielsweise über Smartphones, E-Mails, Websites, Foren, Chats und Communities.

Verschiedene Formen des Mobbing:

- diffamierende Fotos oder Filme
- Lästerei über eine bestimmte Person
- Verbreitung von Unwahrheiten unter falschen Account

Verbreitung in der Öffentlichkeit

Unterschiede Online und Offline

Eingriff rund um die Uhr in das Privatleben

Das Publikum ist unüberschaubar groß; Inhalte verbreiten sich extrem schnell

Bullies können anonym agieren

Betroffenheit des Opfers wird nicht unmittelbar wahrgenommen

Probleme:

- Schnelllebigkeit
- Anonymität & Distanz
- Übermäßiges Mitteilen persönlicher Informationen
- Freunde versus Bekannt

Cyberstalking

Variante 1: Offline
Diese Variante des Cyberstalking beschreibt eben jene Delikte, die es auch **offline** schon gab. Beispiel: Der verschmähte Liebhaber möchte seine Freundin zurückbekommen und schreibt ihr täglich mehrere E-Mails.
Früher tat er das durch Briefe oder zahlreiche Anrufe, nun tut er dies online.

Variante 2: Online
Es werden zum Stalking Applikationen verwendet, die es in der Offline-Variante noch nicht gibt.
Beispiel: Bleiben wir bei dem Liebhaber. Er versucht seine Freundin zurück zu erobern, indem er ihr täglich mehr als 50 WhatsApp-Nachrichten schickt.

Abgrenzungen

Cyber-Mobbing

Cyber-Mobbing, auch Cyber-Bullying genannt ist das absichtliche und über einen längeren Zeitraum anhaltende Beleidigen, Bedrohen, Bloßstellen, Belästigen, Anpöbeln, Tyrannisieren oder Ausgrenzen anderer über digitale Medien. Cyber-Mobbing findet vor allem in Sozialen Netzwerken, Chats, Messengern oder per Handy über SMS, WhatsApp, lästige Anrufe, Handyfotos und -videos statt.

Sexting **"Sexting: es kommt anders als erwartet"**

Sexting ist ursprünglich das Texten, also Schreiben, über sexuelle Themen gewesen, hat sich aber schnell vom Texten zum Senden von Bildern entwickelt. Beim Sexting machen Jugendliche, entweder freiwillig oder durch Mobbing oder Manipulation gezwungen, erotische Fotos des eigenen Körpers und versenden diese über Handys oder Webcams.

Cyber-Grooming

Grooming ist eine spezifische Art der sexuellen Belästigung. Man versteht darunter das sexuell motivierte Anschreiben von Kindern und Jugendlichen durch erwachsene, fremde Personen im Internet.

Cybergrooming

Cybergrooming bezeichnet die Anbahnung von sexueller Gewalt gegen Minderjährige im Internet. Das englische Wort „Grooming“ bedeutet „Striegeln“ und steht metaphorisch für das subtile Annähern von Täter:innen an Kinder und Jugendliche.

CSAM – Wissensgenerierung

Wissensgenerierung (Aufdeckung und Zusammenfassung)

- Bild-Hash-Datenbanken, Foto DNA
- Schlüsselwörter
- Web-Crawler (Einstiegsseiten)
- Erkennung auf Basis von Namen und Metadaten
- visuelle Erkennung

Ergebnisse deuten darauf hin, dass CSAM-Erkennungsanwendungen die besten Ergebnisse liefern, wenn mehrere Ansätze in Kombination verwendet werden.

Die Erstellung eines Täterprofils im Bereich Cybercrime

Differenzierung der Täter nach folgender Typologie

Art der Differenzierung	Beschreibung	Beispiel
Delikt	In der Differenzierung nach Delikten geht es um eine strafrechtliche Unterscheidung. Man betrachtet den juristischen Sachverhalt.	Das Durchführen einen DDoS-Attacke, ist im Sinne des jeweilig zutreffenden Paragraphen des Strafgesetzbuches strafbar.
Formation	In welcher Gruppierung die Tater auftreten. Einzeltäter, Gruppentäter oder Staaten.	Russische und chinesische Betrüger schließen sich zusammen und stehlen online Geld von einer Bank in Australien.
Motiv	Mit welchem Motiv begründet der Täter die Tat. Motive sind extrinsischer (z. B. wirtschaftliche, terroristische) oder intrinsischer (z. B. persönlich, Rache) Natur.	Ein Mitarbeiter stiehlt unternehmensinterne Daten vom Laufwerk eines Vorgesetzten und spielt diese der Konkurrenz zu.
Art des Angriffs	Ungerichtete, gezielete und skalpellartige Angriffe	Ungerichteter Angriff: z. B. ein SPAM-E-Mail erhalten; Gezielter Angriff: z. B. einen Konkurrenten ausspionieren; Skalpellartiger Angnff: z. B. massive Schädigung einer IT-Infrastruktur.
Angriffsort	Klärt von wo aus der Angriff organisiert wird. Inland oder Ausland.	Österreichische User laden sich illegal Videos mit kinderpornografischen Inhalt auf ihren PC.

Den typischen Cyber-Kriminellen gibt es nicht

Mögliche Einteilung A:

- externe Hacker
- Eigene Mitarbeiter im Unternehmen
- Gruppen im Sinne der organisierten Kriminalität
- Cyber-Terroristen
- Staaten als Akteure von Cybercrime-Attacken

Mögliche Einteilung B:

- Cyber-Aktivisten (Hacktivisten)
- Cyber-Kriminelle
- Wirtschaftsspione im Cyber-Raum
- staatliche Nachrichtendienste im Cyber-Raum
- staatliche Akteure im Cyber-War (Militär)
- Cyber-Terroristen
- Skript Kiddies

Hacker, Black-Hat, White-Hat, Cyber-Terroristen

Infos auch nochmal im Lehrbrief

Hacktivismus

Hacktivismus ist Aktivismus, der Techniken des Hackings verwendet, um politische oder soziale Ziele zu fördern. Hacktivisten setzen digitale Angriffe ein, um Missstände aufzuzeigen oder politische Botschaften zu verbreiten.

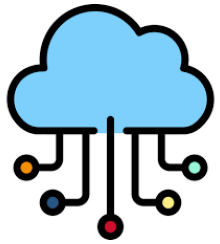
Herausforderungen im Zusammenhang mit Cybercrime

- schnelle technologische Entwicklung
- zeitintensive Gesetzgebungsprozesse
- Industrialisierung von Cybercrime
- Faktor Mensch

„Neue“ Technologien für die breite Masse

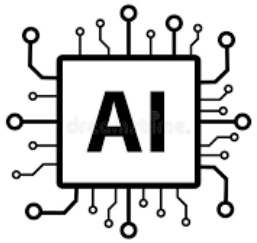
Cloud-Computing

Die Verbreitung von Cloud-Computing-Technologien hat Unternehmen und Einzelpersonen ermöglicht, auf sichere und kostengünstige Weise auf eine Vielzahl von IT-Ressourcen zuzugreifen, ohne eigene physische Infrastruktur betreiben zu müssen. Dies hat die Flexibilität, Skalierbarkeit und Zusammenarbeit verbessert.



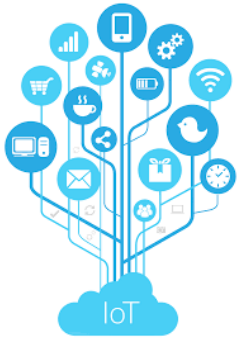
Künstliche Intelligenz und maschinelles Lernen

Fortschritte in den Bereichen künstliche Intelligenz und maschinelles Lernen haben die Entwicklung intelligenter Systeme ermöglicht, die komplexe Aufgaben ausführen können, wie Bilderkennung, Sprachverarbeitung, automatisierte Entscheidungsfindung und persönliche Assistenten wie Siri und Alexa.



Internet der Dinge (IoT)

Die Vernetzung von physischen Geräten und Objekten mit dem Internet hat zu einer neuen Ära des "intelligenten" Wohnens und Arbeitens geführt. Durch IoT können Geräte miteinander kommunizieren und Daten austauschen, um Effizienz zu steigern, Automatisierung zu ermöglichen und neue Dienste bereitzustellen.



Industrialisierung von Cybercrime

- Die Professionalisierung der Cyberkriminalität erreicht 2024 ein neues Niveau der Profitabilität, teilweise durch die Verbreitung von Ransomware-as-a-Service (RaaS).
- Die Anzahl der Opfer von Ransomware-Angriffen hat sich im Vergleich zu 2022 verdoppelt, was zeigt, dass Ransomware immer noch eine der schädlichsten, kostspieligsten und häufigsten Angriffsmethoden im EMEA-Raum ist.
- Es gibt einen klaren Trend zu gezielten Angriffen auf den öffentlichen Sektor und kritische Infrastrukturen, insbesondere im Gesundheits-, Bildungs- und Regierungswesen, aufgrund mangelnder Sicherheitsressourcen in diesen Bereichen.
- Cyberkriminelle nutzen immer aggressivere Ransomware-Methoden, darunter Double-Extortion-Angriffe, bei denen sie sensible Daten verschlüsseln und mit ihrer Veröffentlichung drohen.

Strafrechtlicher Prüfprozess

Prüfprozess

1. Objektiver Tatbestand
2. Subjektiver Tatbestand
3. Rechtswidrigkeit
4. Schuld und Schuldunfähigkeit
5. Ergebnis der Strafbarkeit

Prüfprozess

1. Objektiver Tatbestand

- Prüfung der Tatbestandsmerkmale
- Begriffsauslegung
- Subsumtion
- Ergebnis

→ Falls alle relevanten TBM erfüllt, dann weiter mit subjektivem Teil

Prüfprozess

2. Subjektiver Tatbestand

- Bewusstsein des Täters während der Tat (innere Haltung des Täters)
- Vorsatz oder Fahrlässigkeit (§ 15 StGB)
  - Vorsatz: Wissen und Wollen der Tatbestandsverwirklichung mit allen seinen Umständen
  - Fahrlässigkeit: Tatbestandsverwirklichung unter einer objektiven Sorgfaltspflichtverletzung bei objektiver Vorhersehbarkeit des Erfolgseintritts/Schaden
- Subsumtion
- Ergebnis

→ Falls erfüllt, dann weiter mit Rechtswidrigkeit

Prüfprozess

3. Rechtswidrigkeit

- Rechtfertigungsgründe vorhanden?
  - Notwehr oder Nothilfe (§ 32 StGB)
  - Rechtfertigender Notstand (§ 34 StGB)
  - Festnahmerecht (§ 127 StPO) etc.

→ Falls nicht erfüllt, dann weiter mit Schuld und Schuldunfähigkeit

Prüfprozess

4. Schuld und Schuldunfähigkeit

- Schuldausschließungsgründe vorhanden?
  - Schuldunfähigkeit des Kindes (§ 19 StGB)
  - Schuldunfähigkeit wegen seelischer Störungen (§ 20 StGB)
  - Verminderte Schuldunfähigkeit (§ 21 StGB)

→Falls nicht erfüllt, dann weiter mit dem Ergebnis der Strafbarkeit

Vielen Dank

Prof. Dr. rer. nat. Dirk Labudde

Hochschule Mittweida | University of Applied Sciences
Technikumplatz 17 | 09648 Mittweida
Fakultät Computer- und Biowissenschaften | Fraunhofer Lernlabor

T +49 (0) 3727 58-1469
F +49 (0) 3727 58-21469

dirk.labudde@hs-mittweida.de

Haus 8 | Richard Stücklen-Bau | Raum 8-105
Am Schwanenteich 6b | 09648 Mittweida

HOCHSCHULE MITTWEIDA
University of Applied Sciences

hs-mittweida.de