Lehr- und Studienbriefe
Kriminalistik / Kriminologie

Band
26

Keller • Braun • Roggenkamp

Cybercrime

VERLAG DEUTSCHE POLIZEILITERATUR GMBH
Buchvertrieb

Lehr- und Studienbriefe Kriminalistik / Kriminologie

Herausgegeben von
Horst Clages, Leitender Kriminaldirektor a.D.,
Wolfgang Gatzke, Direktor LKA NRW a.D.

Band 26
Cybercrime

von
Christoph Keller, Polizeidirektor
Prof. Dr. Frank Braun
Prof. Dr. Jan Dirk Roggenkamp

VERLAG DEUTSCHE POLIZEILITERATUR GMBH
Buchvertrieb

Bibliographische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliographie; detaillierte bibliographische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

E-Book
1. Auflage 2020

ISBN 978-3-8011-0881-6 (EPUB)

Buch (Print)
1. Auflage 2020

Satz: VDP GMBH Buchvertrieb, Hilden
Druck und Bindung: Druckerei Hubert & Co, Göttingen
Printed in Germany
ISBN 978-3-8011-0880-9

Satz und E-Book: VDP GMBH Buchvertrieb, Hilden

E-Mail: service@vdpolizei.de

Vorwort

Unter dem schillernden Begriff Cybercrime wird eine Vielzahl unterschiedlichster Straftaten verstanden, deren kleinster gemeinsamer Nenner die kriminelle Nutzung von Informationstechnologie und IT-Strukturen, namentlich des Internets ist. Cybercrime-Phänomene reichen vom Hacking über den betrügerisch-destruktiven Einsatz von Malware und Botnetzen, Angriffe auf den Zahlungs- und Warenverkehr mittels Phishing- und Skimming-Methoden oder das Bereitstellen und die Nutzung krimineller Infrastruktur im sog. Darknet.

Diese Einführung orientiert sich an den unterschiedlichen Erscheinungsformen von Cybercrime. Die Identifizierung der typischen kriminellen Handlungsmuster (Teil A.) ist demnach Ausgangspunkt der Darstellung, wobei auf die einschlägigen Straftatbestände hingewiesen wird. Daran schließt sich ein knapper Überblick über die wichtigsten strafrechtlichen Fragestellungen an (Teil B.). In den nachfolgenden Kapiteln stehen die Ermittlungsmöglichkeiten der Strafverfolgungsbehörden im Fokus (Teil C. Computerforensik und Teil D. Informationsgewinnung in Netzwerken), gefolgt von Handlungsanweisungen zur Kriminalitätsbekämpfung im sog. Ersten Angriff (Teil E. Polizeiliche Bekämpfung der Internetkriminalität). In einem Ausblick wird zudem auf den ermittlungstechnischen Einsatz von Big-Data-Technologie (Teil F.) aufmerksam gemacht.

Als Einführungswerk richtet sich die Schrift in erster Linie an Praktiker, die einen „Neueinstieg“ in die Materie suchen, sowie an Polizeibeamte in Ausbildung und Studium. Für eine Vertiefung der gewonnenen

Erkenntnisse sei insbesondere auf das Handbuch von Dieter Kochheim, Cybercrime und Strafrecht in der Informations- und Kommunikationstechnik, 2. Aufl. 2018, und dessen Internetauftritt (http://www.cyberfahnder.de) hingewiesen.

Zu danken gilt es Herrn EKHK Ulli Bahlo und Herrn EKHK Peter Niehoff für die kritische Durchsicht des Manuskripts und ihre wertvollen Hinweise, die vor allem bei der Erstellung von Checklisten Eingang in die Darstellung gefunden haben.

Berlin, Hofkirchen und Mettingen im Sommer 2020

Die Autoren

Inhaltsverzeichnis

11. Skimming
12. Carding
13. Kontaktloses Bezahlen/NFC-Betrug
14. Abo-Fallen
15. Cybermobbing/Cyber-Bullying
16. Happy Slapping
17. Sextortion
18. Romance-Scamming
19. Darstellung des sexuellen Missbrauchs von Kindern (sog. Kinderpornografie)
20. Cybergrooming
21. Kryptowährungen/Bitcoins
    a) Funktionsweise
    b) Kriminalitätsphänomene
    c) Einziehung und Beschlagnahme von Bitcoins
22. Urheberrecht
    a) Filesharing, Tauschbörsen
    b) Streaming

B. Materielles Strafrecht (Überblick)

I. Verbreitungs- und Äußerungsdelikte

1. Verbreitungsdelikte
2. Äußerungsdelikte
    a) Straftatbestände
    b) Strafbarkeitsfragen bei Beleidigung und Volksverhetzung
3. Verantwortlichkeit der Provider

A. Phänomenologie

I. Unrechtskultur im digitalen Raum

Die Digitalisierung in allen Bereichen bietet umfassende Möglichkeiten für Straftäter

Viele „klassische“ Deliktsfelder werden zu einem nicht unerheblichen Teil in der „digitalen Welt“ abgewickelt. So wird im Internet illegal Handel mit Betäubungsmitteln, Waffen, Darstellungen des sexuellen Missbrauchs von Kindern sowie urheberrechtlich geschütztem Material betrieben. Die Betrugsfälle im Netz – von „Abo-Fallen“ bis zum millionenschweren Anlagebetrug bei Kryptowährungen[1] – sind seit jeher Legion. Höchstes Schadenspotential bergen Angriffe auf die Vertraulichkeit und Integrität informationstechnischer Systeme[2]. Gerade durch die Manipulation von IT-Systemen bzw. deren Sabotage (etwa durch Bot-Netze, Einsatz von Ransomware, Hacking) können die Funktionsfähigkeit von Wirtschaft und Staat gefährdet werden.

Der Begriff **Cybercrime** bezeichnet als Sammelbegriff alle Straftaten, die sich gegen das Internet, Datennetze, informationstechnische Systeme oder deren Daten richten (Cybercrime im engeren Sinne) oder die mittels dieser Informationstechnik begangen werden.[3] Es handelt sich um einen äußerst dynamischen Deliktsbereich, dem im Zuge der umfassenden Digitalisierung neue Kriminalitätserscheinungen hinzutreten. Das Spektrum ist nahezu unbegrenzt und reicht u.a. von Hacking-Attacken, Verbreitung und Einsatz von Schadsoftware, über

Kreditkartenbetrug, Urheberrechtsverletzungen, bis hin zu Identitätsdiebstahl und Cyber-Terrorismus bzw. Cyber-War.[4]

Die Kreativität der Delinquenten kennt dabei kaum Grenzen. Auf technische Entwicklungen wird flexibel, schnell und professionell reagiert, etwa bei der Verbreitung von Malware[5]. Befeuert wird dies durch eine kriminelle Wissenscommunity, die sich in der „Underground economy“ (dt. „Schwarzmarkt“ – bezogen auf entsprechende Foren und Plattformen im sog. Darknet)[6] etabliert hat. Dort werden Themen wie das Programmieren von Malware diskutiert oder Anleitungen zum Hacken von Webservern und Hinweise zum Anmieten von Bot-Netzen gegeben. Technisch weniger Begabte können „gephishte“ Zugangsdaten zu Bank-, eBay- oder PayPal-Konten oder „geskimmte“ oder sonst entwendete Kreditkarten-Daten (sog. „credit card dumps“) usw. käuflich erwerben.[7]

Die Tätertypen sind, wie ihre Motive und ihr technisches Können, äußerst different.[8] Vom „Einsteiger bis zum Profi“ ist alles vertreten: jugendliche Hacker, die ihr Potenzial testen wollen, Gelegenheitstäter, Extremisten, Erpresser, Terroristen, lose kriminelle Zusammenschlüsse und international organisierte Banden, Nachrichtendienste anderer Staaten, usw. Im Bereich des Hacking werden vom BKA grob folgende Typen unterschieden:[9]

Einsteiger	Kriminelle mit IT-Grundkenntnissen. Z.B. sog. Script Kids, die sich mittels Software-Toolkits überwiegend mit Phishing im Bereich Social Engineering und oder Defacement beschäftigen, also dem Verändern von Webseiten.
Hacker (Fortgeschrittene)	Führen strukturierte Attacken durch, wie DDoS, Drive-by-exploits oder SQL-injections
Profis	Staatlich gelenkte Hacker, terroristische

	Gruppen oder auch „Hacktivisten“; Hacktivisten verstehen sich als Kämpfer gegen Ungerechtigkeit (Handeln als ziviler Ungehorsam gegen bestimmte politische Richtungen)

Bei der Bekämpfung dieser äußerst breit gefächerten IT-Kriminalität sind generalpräventive Aspekte als nachrangig zu bewerten. Zwar erfolgt in regelmäßigen Abständen reflexartig der Ruf nach dem Strafrecht („Strafrecht als politischer Reflex“[10]) kombiniert mit der Floskel, dass das „Internet kein rechtsfreier Raum“[11] sein oder werden dürfe. Übersehen wird hierbei, dass das Strafrecht bereits seit vielen Jahren einen weitgehend geeigneten Deliktskatalog mit angemessenen Strafrahmen zur Verfügung stellt (allgemeine Straftatbestände[12] und spezielle zur Bekämpfung der „Computerkriminalität“, vgl. **B.**). Zudem zeigen Untersuchungen zur negativen Generalprävention, dass im Bereich Cybercrime die erwartete Schwere der Strafe bedeutungslos ist. Die Verschärfung des Rechts würde also kaum Auswirkungen haben. Es gibt keine Anhaltspunkte dafür, dass eine Verschärfung des Strafrechts das Normbewusstsein positiv beeinflussen würde[13]. Zu adressieren ist vielmehr das von (potentiellen) Tätern wahrgenommene Entdeckungsrisiko. Im digitalen Raum herrscht offenbar nur geringe Angst vor Strafverfolgung. Anders gewendet: Die bestehenden Straftatbestände kommen mangels adäquater Verfolgung nicht zur Anwendung. Strategisch muss deshalb die Erhöhung der Verfolgungswahrscheinlichkeit im Mittelpunkt stehen. Gerade den Sicherheitsbehörden kommt bei der Bekämpfung der Unrechtskultur im digitalen Raum eine wichtige Rolle zu.[14] Um dieser gerecht werden zu können, bedarf es zunächst auf breiter Basis phänomenologischer Kenntnisse. Nachfolgend werden

daher die für die Praxis wichtigsten Phänomene des Cybercrime in ihren Grundzügen dargestellt.

II. Kriminalitätsbegriff und Kriminalitätserfassung

1. Cybercrime-Konvention

Das „Übereinkommen über Computerkriminalität“ – besser bekannt als **„Convention on Cybercrime“** bzw. **Cybercrime-Konvention** – ist ein Übereinkommen des Europarats aus dem Jahr 2001.[15] Sie wurde ausgehandelt, um dem grenzüberschreitenden Charakter der Kriminalität im Internet Rechnung zu tragen. Die Gesamtzahl der Ratifikationen bzw. Beitritte beläuft sich derzeit auf 64 Staaten.[16] Zweck des Abkommens ist eine wirksame internationale Zusammenarbeit bei der Bekämpfung der Datennetzkriminalität. Verbesserten Schutz vor IT-Kriminalität sollen dabei harmonisierte Straftatbestände schaffen. In dem Abkommen sind Vorgaben für konkrete Straftatbestände enthalten, die es auf nationaler Ebene zu schaffen gilt. Folgende Kategorien nennt die Cybercrime-Konvention:

(1) **Straftaten gegen die Vertraulichkeit, Unversehrtheit und Verfügbarkeit von Computerdaten und -systemen** (Kap. 1, Abschn. 1, Titel 1 Cybercrime-Konvention)

- Ausspähen und Abfangen von Daten, Datenveränderung, Computersabotage einschließlich Vorbereitungshandlungen, Infizierung von Computersystemen mit Schadsoftware, Datenspionage-Hacking, Phishing, Störung des Zugriffs auf Computersysteme, Herstellen, Verschaffen und Zugänglichmachen von

Passwörtern, Sicherungscodes oder auf die Begehung von Straftaten abzielender Computerprogramme, hacking tools, crimeware

(2) **Computerbezogene Straftaten** (Kap. 1, Abschn. 1, Titel 2 Cybercrime-Konvention)

– betrügerische Angriffe auf das Vermögen, Betrug, Computerbetrug, bei denen im Einzelfall aber auch die missbräuchliche Verwendung der digitalen Identität eines anderen und damit der Tatbestand des Verfälschens und Gebrauchens beweiserheblicher Daten eine Rolle spielen kann. Außerdem geht es hier um Angriffe auf höchstpersönliche Rechtsgüter wie die Ehre, Cybermobbing, Cyberbullying.

(3) **Inhaltsbezogene Straftaten** (Kap. 1, Abschn. 1, Titel 3 Cybercrime-Konvention)

– Straftaten, bei denen über das Netz illegale Inhalte transportiert werden, also Informationen, mit denen der Umgang vom Gesetzgeber mit Strafe bedroht wird, z.B. Darstellung des sexuellen Missbrauchs von Kindern, Gewaltdarstellungen und Propagandadelikte

(4) **Straftaten im Zusammenhang mit Verletzungen des Urheberrechts und verwandter Schutzrechte** (Kap. 1, Abschn. 1, Titel 4 Cybercrime-Konvention)

– unerlaubte Verwertung urheberrechtlich geschützter Werke, unerlaubtes Verbreiten von Bildnissen, z.B. unbefugtes Herunterladen und Verbreiten von Musik, Filmen, Software mittels Filesharing-Systemen oder Peer to Peer-Netzwerken wie eMule oder BitTorrent

(5) Mittels Computersystemen begangene **Handlungen rassistischer und fremdenfeindlicher Art** (Zusatzprotokoll zur Cybercrime-Konvention v. 28.1.2003, sog. Antirassismus-Abkommen)[17]

Derzeit wird ein weiteres Zusatzprotokoll zur Cybercrime-Konvention beraten, das den grenzüberschreitenden Zugriff der Strafverfolgungsbehörden auf Daten zum Gegenstand hat. Ein entsprechender Entwurf wird in Kürze erwartet.

Insbesondere Brasilien, China und Russland stehen dem Übereinkommen aus unterschiedlichen Gründen ablehnend gegenüber, was bedeutet, dass mehr als 50 Prozent des internationalen Internetverkehrs nicht erfasst werden.[18]

2. Cybercrime

Vor dem Hintergrund internationaler sicherheitspolitischer Entwicklungen wurden der phänomenbezogene Sprachgebrauch harmonisiert und die Sachverhalte, die bislang unter den Terminus „IuK-Kriminalität“ gefasst wurden, durch den Begriff „Cybercrime“ ersetzt. Im **Bundeslagebild Cybercrime** des BKA (2017) wird dieser Deliktsbereich allgemein wie folgt definiert:

> „Cybercrime umfasst die Straftaten, die sich gegen das Internet, weitere Datennetze, informationstechnische Systeme oder deren Daten richten. Cybercrime umfasst auch solche Straftaten, die mittels dieser Informationstechnik begangen werden.“[19]

Es wird weiter zwischen **Cybercrime im engeren und im weiteren Sinne** differenziert: Neben spezifischen Angriffen auf informationstechnische Systeme (Angriffsobjekt = Daten), die mittels hierfür geschaffener

Datendelikte sanktioniert werden (Cybercrime im engeren Sinne), wird auch die Nutzung derartiger Systeme zur Tatbegehung – sowohl als Tatmittel, wie auch als Angriffsmedium – erfasst (Cybercrime im weiteren Sinne).[20]

a) Cybercrime im engeren Sinne

Zentrale Schutzgüter der unter Cybercrime im engeren Sinne gefassten Straftatbestände sind die Integrität und die Vertraulichkeit informationstechnischer Systeme.[21]

Erscheinungsformen von Cybercrime im engeren Sinne sind vor allem:[22]

- Einsatz von Schadprogrammen, z.B. „Malware“ und Trojaner, als Tatmittel zum Angriff auf informationstechnische Systeme (unten **III. 6.**)
- Kriminelle Nutzung sogenannter „Botnetze“ (unten **III. 1.**)
- Überlastung von Servern („DDoS-Angriffe“, unten **III. 2.**) und
- unberechtigtes Eindringen in Rechnersysteme („Hacking“ unten **III. 3.**).

Cybercrime im engeren Sinne umfasst im Wesentlichen folgende **Delikte**:[23]

- Ausspähen und Abfangen von Daten einschließlich Vorbereitungshandlungen und Datenhehlerei (§§ 202a, 202b, 202c, 202d StGB)
- Fälschung beweiserheblicher Daten bzw. Täuschung im Rechtsverkehr (§§ 269, 270 StGB)
- Datenveränderung/Computersabotage (§§ 303a, 303b StGB)

− Computerbetrug (§ 263a StGB)

Die Zuordnung einzelner Delikte zur Gruppe Cybercrime im engeren Sinne ist zum Teil strittig. So wird der Computerbetrug nach § 263a StGB auch zur Cybercrime im weiteren Sinne gezählt.[24]

Bei den aufgeführten Straftatbeständen ist eine zweigliedrige Regelungsstruktur erkennbar. Die §§ 202a ff. StGB pönalisieren den **Zugriff auf fremde Daten**, begonnen mit dem zweckgerichteten Vorhalten von Spähsoftware, bis hin zum mit dem Tatbestand der Datenhehlerei (§ 202d StGB) pönalisierten Ankauf widerrechtlich erlangter Daten. Regelungstechnisch getrennt hiervon steht das **Verändern von Daten** in den §§ 303a f. StGB. Dabei nimmt der Gesetzgeber sowohl den Persönlichkeitsrechtsschutz in den Blick, als auch die vermögensrechtliche Bedeutung von Daten.[25]

b) Cybercrime im weiteren Sinne

Während die Begehung der vorgenannten Delikte eine gewisse Technikaffinität voraussetzt, beschreibt der Terminus **Cybercrime im weiteren Sinne** die (traditionellen) Deliktsbereiche, bei denen informationstechnische Systeme zur Tatbegehung genutzt werden[26], also Straftaten, die im oder mit Hilfe des Internets begangen werden.

Es handelt sich um Straftatbestände, die regelmäßig auch im realen Raum verwirklicht werden können, wie Betrugsstraftaten, verbotenes Glücksspiel oder Verbreitung von sog. Kinderpornografie (korrekt: Darstellung des sexuellen Missbrauchs von Kindern).[27] Insbesondere sind folgende Straftatbestände relevant: Volksverhetzung (§ 130 StGB), Anleitungen zu Straftaten (§ 130a StGB),

Gewaltdarstellung (§ 131 StGB), Verbreitung pornographischer Schriften (§ 184 StGB), Verbreitung gewalt- oder tierpornographischer Schriften (§ 184a StGB), Verbreitung, Erwerb und Besitz „kinderpornographischer“ Schriften (§ 184b StGB), Verbreitung, Erwerb und Besitz jugendpornographischer Schriften (§ 184c StGB), Ehrverletzungsdelikte (§§ 185 ff. StGB), Verletzung des höchstpersönlichen Lebensbereichs durch Bildaufnahmen (§ 201a StGB), Betrug (§ 263 StGB), Unerlaubte Veranstaltung eines Glückspiels (§ 284 StGB) und die Beteiligung daran (§ 285 StGB).

3. Dokumentation von Cybercrime

In der **Polizeilichen Kriminalstatistik** (PKS) werden Cybercrime-Delikte in der Rubrik „Tatmittel“ mit dem Schlagwort „Internet“ erfasst:

Schlüsselzahl 516300	Betrug mittels rechtswidrig erlangter Debitkarten mit PIN, § 263a StGB
Schlüsselzahl 517500	Computerbetrug, § 263a StGB
Schlüsselzahl 517902	Computerbetrug mit Zugangsberechtigungen zu Kommunikationsdiensten, §§ 263, 263a StGB
Schlüsselzahl 516502	Computerbetrug mittels rechtswidrig erlangter Daten von Zahlungskarten, §§ 253, 263a StGB
Schlüsselzahl 543000	Fälschung beweiserheblicher Daten, § 269 StGB
Schlüsselzahl 516502	Computerbetrug mittels rechtswidrig erlangter Daten von Zahlungskarten, §§ 253, 263a StGB
Schlüsselzahl 543000	Fälschung beweiserheblicher Daten, § 269 StGB
Schlüsselzahl 543001	Täuschung im Rechtsverkehr bei Datenverarbeitung, § 270 StGB
Schlüsselzahl 674200	Datenveränderung, Computersabotage, §§ 303a, 303b StGB
Schlüsselzahl 678000	Ausspähen von Daten, § 202a StGB
Schlüsselzahl 678020	Abfangen von Daten, § 202b StGB
Schlüsselzahl 678030	Vorbereitungshandlungen zu §§ 202a, 202b, 202c

	StGB
Schlüsselzahl 674200	Datenveränderung, § 303a StGB
Schlüsselzahl 674201	Computersabotage, § 303b StGB
Schlüsselzahl 715100	Softwarepiraterie (private Anwendung z.B. Computerspiele)
Schlüsselzahl 715200	Softwarepiraterie in Form gewerbsmäßigen Handelns.

Aus den Zahlen der **PKS** generiert das Bundeskriminalamt das „**Bundeslagebild Cybercrime**“. Im Berichtszeitraum eines Jahres beschreibt das Lagebild das Gefahren- und Schadenspotenzial von Cybercrime und deren Bedeutung für die Kriminalitätslage in Deutschland.

Die Entwicklung der Cybercrime stellt sich 2018 danach wie folgt dar:[28]

- 87.106 Fälle von Cybercrime im engeren Sinne (+1,3%)
- 271.864 Fälle mit dem Tatmittel Internet unter allen in der PKS erfassten Straftaten (4,9% aller in der PKS erfassten Straftaten)
- 723 Fälle von Phishing im Online-Banking (-49%)
- 60,7 Mio. Schaden im Bereich Computerbetrug (2017: 71,4 € Mio. Schaden)
- 13 OK-Gruppierungen im Kriminalitätsbereich Cybercrime[29]; 2,4% aller OK-Verfahren (2017: 17).

Zur Optimierung des Informationsaustauschs wurde 2011 das **Nationale Cyber-Abwehrzentrum** gegründet, das als Kooperationsplattform für staatliche und private Akteure fungiert und so die Bildung eines einheitlichen Lagebilds erleichtert. Der 2012 gegründete private **Cyber-Sicherheitsrat e.V.** versteht sich als Wissensplattform für private und staatliche Akteure; er berät auch das Nationale Cyber-Abwehrzentrum.[30]