

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

© VERLAG DEUTSCHE POLIZEILITERATUR GMBH Buchvertrieb, Hilden
Keller • Braun • Roggenkamp, Lehr- und Studienbrief Band 26
„Cybercrime“, 1. Auflage 2020
ISBN 978-3-8011-0880-9

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.

www.vdpolizei.de

1. Auflage 2020

© VERLAG DEUTSCHE POLIZEILITERATUR GMBH Buchvertrieb; Hilden/Rhld., 2020

Alle Rechte vorbehalten

Satz: VDP GMBH Buchvertrieb, Hilden

Druck und Bindung: Druckerei Hubert & Co, Göttingen

Printed in Germany

ISBN 978-3-8011-0880-9

© VERLAG DEUTSCHE POLIZEILITERATUR GMBH Buchvertrieb, Hilden

Keller • Braun • Roggenkamp, Lehr- und Studienbrief Band 26

„Cybercrime“, 1. Auflage 2020

ISBN 978-3-8011-0880-9

Inhaltsverzeichnis

Vorwort	3
A. Phänomenologie	11
I. Unrechtskultur im digitalen Raum	11
II. Kriminalitätsbegriff und Kriminalitätserfassung	13
1. Cybercrime-Konvention	13
2. Cybercrime.....	14
a) Cybercrime im engeren Sinne.....	14
b) Cybercrime im weiteren Sinne	15
3. Dokumentation von Cybercrime	16
4. Dunkelfeldproblematik	17
III. Phänomene.....	18
1. Botnetze und Cybercrime as a service.....	18
2. DDoS-Angriffe.....	20
3. Hacking	21
4. Seitenkanalangriffe	22
5. Strafbares Verhalten von Chatbots/Socialbots	22
a) Chatbots	22
b) Socialbots	23
6. Malware/Ransomware/Scareware	24
7. Phishing	26
8. Pharming	27
9. Social Engineering/Spear-Phishing/Whaling.....	27
10. Identitätsdiebstahl	28
11. Skimming.....	28
12. Carding.....	30
13. Kontaktloses Bezahlen/NFC-Betrug	30
14. Abo-Fallen.....	31
15. Cybermobbing/Cyber-Bullying.....	32
16. Happy Slapping	35
17. Sextortion.....	35
18. Romance-Scamming	35

19.	Darstellung des sexuellen Missbrauchs von Kindern (sog. Kinderpornografie).....	36
20.	Cybergrooming.....	37
21.	Kryptowährungen/Bitcoins	38
a)	Funktionsweise.....	39
b)	Kriminalitätsphänomene	40
c)	Einziehung und Beschlagnahme von Bitcoins.....	41
22.	Urheberrecht.....	41
a)	Filesharing, Tauschbörsen.....	43
b)	Streaming.....	43
B.	Materielles Strafrecht (Überblick)	45
I.	Verbreitungs- und Äußerungsdelikte	46
1.	Verbreitungsdelikte.....	47
2.	Äußerungsdelikte	47
a)	Straftatbestände.....	47
b)	Strafbarkeitsfragen bei Beleidigung und Volksverhetzung	47
3.	Verantwortlichkeit der Provider.....	49
4.	Inkurs: Die Regelungen des Netzwerkdurchsetzungsgesetzes (NetzDG)	50
II.	Delikte zum Schutz der Intim- und Privatsphäre	52
III.	IT-spezifische Straftatbestände	53
1.	Schutz der Datenintimität: Strafbarer Datenzugriff (§§ 202a-c StGB)	53
2.	Schutz der Datenintegrität: Datenveränderung und Computersabotage § 303a, b StGB	54
3.	Schutz des Vermögens und des Rechtsverkehrs: Computerbe- trug, Fälschung beweisbarer Daten und Täuschung im Rechtsverkehr bei Datenverarbeitung (§§ 263a, 269, 270 StGB)	55
IV.	E-Commerce-Delikte	56
V.	Sonstige Straftatbestände.....	56
VI.	Nebenstrafrecht	57
VII.	Straftaten mit Auslandsbezug	57
1.	Territorialitätsprinzip	57

2.	Ausnahmsweise Anwendung des deutschen Strafrechts auf Auslandstaten	58
3.	Problem: Grenzüberschreitende Distanzdelikte.....	59
C.	Computerforensik	61
I.	Strafprozessuale Grundlagen	62
1.	Sicherstellung und Beschlagnahme von Daten	62
2.	Zugriff auf E-Mails	62
3.	Durchsicht von Daten und Zugriff auf Cloud-Speicher.....	64
a)	Grundlagen	64
b)	Zugriff auf Cloud-Speicher.....	65
aa)	Im Ausland gespeicherte Daten.....	66
bb)	„Loss of location“/„good-faith“	67
4.	Online-Durchsuchung	68
5.	Quellen-TKÜ.....	69
6.	DSL-Überwachung	70
II.	Sicherstellung digitaler Beweismittel bei Wohnungsdurchsuchungen.....	71
III.	Sicherung elektronischer Beweismittel.....	72
IV.	Datensicherung, Spurensicherung	73
V.	Sicherstellung von Mobiltelefonen, Smartphones	73
1.	Vorgehensweise	75
2.	Zwangsweise Entsperrung biometrisch gesicherter Smartphones.....	75
VI.	Auswertung, Untersuchung inkriminierter Geräte	76
1.	Beweiswertsicherung: Grundsatz der Datenintegrität	76
2.	Beweiswertproblematik bei Online-Durchsuchung und Quellen-TKÜ.....	77
D.	Polizeiliche Informationsgewinnung in Netzwerken	79
I.	Ermittlungen in Sozialen Netzwerken	79
1.	Vorstufe: Ungezieltes Sammeln von Informationen.....	79
2.	Stufe 1: Passives „Ansurfen“ frei zugänglicher Inhalte	80
3.	Stufe 2: Gezielte längerfristige passive „Beobachtung“ virtueller Aktivitäten	81
4.	Stufe 3: Aktive Teilnahme/Kontaktaufnahme (unter „Legende“/Fake-Account).....	82

5.	Alternativen.....	83
II.	Ermittlungen im Darknet	84
1.	Ermittlungsansätze	86
2.	Verdeckte personale Ermittlungen (VE, noeP).....	87
3.	Recherche in öffentlich zugänglichen Quellen – Open Source Intelligence.....	87
4.	Übernahme digitaler Identitäten langjähriger Szene-Mitglieder	87
5.	Längerfristige Beobachtung relevanter Darknet-Plattformen	88
6.	Sicherung relevanter Daten der Verkaufsgeschäfte & Transaktionen.....	88
7.	Analyse von Informationen und Daten	89
8.	Kooperation mit Logistik-Dienstleistern	89
9.	Ausblick.....	89
E.	Polizeiliche Bekämpfung der Internetkriminalität: Erster Angriff und grundlegende Ermittlungsansätze	91
I.	Erforderliche Fachkompetenz.....	91
II.	Polizeiliche Ermittlungsarbeit – Handlungsebenen.....	92
1.	Anlassunabhängige Internetrecherchen	93
2.	Aufnahme einer Strafanzeige (Erster Angriff)	93
3.	Sachbearbeitung	96
4.	Spezielle IT-Beweissicherung (Computerforensik).....	96
III.	Allgemeine Ermittlungsansätze	97
1.	Ermittlungen zur E-Mail	97
2.	Ermittlungen zur IP-Adresse.....	99
3.	Ermittlungen zur Domain.....	100
4.	Auskunftsersuchen an die Provider – Bestandsdatenauskunft	102
a)	Rechtsgrundlagen.....	102
b)	Auskunft zu einer dynamischen IP-Adresse.....	103
c)	Auskunft über Zugangssicherungs_codes.....	104
5.	Vorratsdatenspeicherung/Zugriff auf Verkehrsdaten	105
6.	IP-Tracking, IP-Catching	106
IV.	Ermittlungsansätze in bestimmten Phänomenbereichen	107

1.	Verbotene Inhalte im Internet.....	107
2.	Verbreitung von Gewaltvideos.....	108
3.	Phishing	108
4.	Skimming.....	109
V.	Zusammenarbeit mit der Justiz.....	110
VI.	Internationale Cyber-Ermittlungen	111
F.	Einsatz von Big-Data-Technologie	113
I.	OSINT	113
II.	Predictive Policing	113
III.	Rechtliche Fragestellungen.....	114
	Literaturverzeichnis	115
	Zu den Autoren	124
	Stichwortverzeichnis	125