Cyberkriminalität

Übersicht zu aktuellen und künftigen Erscheinungsformen

Barbara Horten¹ · Marleen Gräber¹

Eingegangen: 13. Mai 2020 / Angenommen: 27. Mai 2020 / Online publiziert: 16. Juni 2020
© Der/die Autor(en) 2020

Zusammenfassung

Die Möglichkeiten für Cyberkriminelle und die Erscheinungsformen von Cyberkriminalität haben durch die Digitalisierung und Verbreitung internetfähiger Geräte in den letzten Jahren stark zugenommen. Unter dem Begriff Cybercrime oder auch Internetkriminalität werden Taten subsumiert, die mittels Internet begangen werden. Es gibt zahlreiche Erscheinungsformen, die je nach Kontext unterschiedlich klassifiziert werden. Die Verbreitung von cyberkriminellen Straftaten wird jährlich im Bundeslagebericht des Bundeskriminalamts (BKA) dargestellt. In diesem werden Herausforderungen u. a. durch neue Methoden der Verbreitung von Malware und des Identitätsdiebstahls benannt. Auch digitale Erpressung, ein vermehrtes Gefahrenpotenzial durch das „Internet der Dinge“ und Angriffe auf die sog. kritischen Infrastrukturen sind als cyberkriminelle Bedrohungen zu sehen. Zudem verbreiten sich sexuell motivierte Straftaten wie z. B. Kinderpornografie schneller im virtuellen Raum. In der *Polizeilichen Kriminalstatistik (PKS)* 2019 wurde ein Anstieg von Cyberkriminalität im Vergleich zum Vorjahr um 15,4 % registriert. Es wird eine Zunahme des Identitätsdiebstahls via Plattformen wie dem Darknet und ein wachsendes Gefährdungspotenzial durch Entwicklungen wie etwa Smart Homes, Cloud Computing oder Big Data prognostiziert. Empirische Studien zu den Viktimisierungserfahrungen von Cyberangriffen liegen zu Privatpersonen und Industrieunternehmen vor. Die Täter waren meist junge, männliche Erwachsene.

Schlüsselwörter Internetkriminalität · Entwicklungstrend · Beschuldigte · Darknet · Malware

✉ Barbara Horten, M.A.
horten@krimi.uni-heidelberg.de

¹ Institut für Kriminologie, Universität Heidelberg,
Friedrich-Ebert-Anlage 6–10, 69117 Heidelberg, Deutschland

Cybercrime

Overview of current and future manifestations

Abstract

The possibilities for cybercriminals and the manifestations of cybercrime have significantly increased in recent years due to the digitalization and spread of internet-enabled devices. The term cybercrime describes criminal acts committed via internet, but there are numerous manifestations which are classified differently depending on the context of cybercrime. The prevalence of cybercrime is presented in the annual Federal Management Report of the German Federal Criminal Police Office (BKA). This report identifies challenges by, among others, new methods of distributing malware and identity theft. Ransomware, an increased danger potential from the Internet of things and attacks on so-called critical infrastructures must also be perceived as cybercriminal threats. In addition, sexually motivated crimes, such as child pornography, also spread faster in the virtual space. The German Police Crime Statistics for 2019 showed a 15.4% increase in cybercrime compared to the previous year. An increase in identity theft via platforms, such as darknet as well as a growing potential threat from developments, such as smart homes, cloud computing or big data is predicted. Empirical studies on the victimization experiences of cyberattacks are available for private individuals and industrial companies. The offenders were mostly young male adults.

Keywords Internet crime · Trend in development · Offenders · Darknet · Malware

Einleitung

Seit dem Beginn des 20. Jh. nimmt die Digitalisierung weltweit stetig an Bedeutung zu. E-Mails, Kommunikationsplattformen, Onlinebanking und andere internetbasierte Techniken haben den Alltag und die Wirtschaft längst durchdrungen und sind aus der modernen Gesellschaft nicht mehr wegzudenken. Jedoch zeichnet sich mit den wachsenden Möglichkeiten des digitalen Wandels zugleich ein Anstieg von Gefahren für Wirtschaft, Staat und Privatpersonen ab. Durch die zunehmende Verbreitung von Computersystemen, Smartphones und anderen internetfähigen Geräten und die vermeintliche Anonymität im Internet werden Cyberangriffe begünstigt. Die Täter haben das Potenzial des Internets zeitgleich mit dessen Verbreitung für ihre Zwecke erkannt und entwickeln nahezu parallel zu den neuesten Sicherheitstechniken Möglichkeiten, die Technik für ihre missbräuchlichen Zwecke zu nutzen. Die Folgen sind wirtschaftliche Schäden im Millionenbereich und gravierende Folgen für einzelne von Internetkriminalität betroffene Personen und Unternehmen, die sich aus dem Diebstahl persönlicher und vertraulicher Daten ergeben.

Der vorliegende Artikel befasst sich mit aktuellen und künftigen Erscheinungsformen der Cyberkriminalität. Hierfür wird zunächst eine definitorische Eingrenzung des Begriffs vorgenommen, um im Anschluss die einzelnen Phänomene dieses Deliktbereichs zu veranschaulichen. Daran schließen ein Überblick zu der Verbreitung von Cybercrimedelikten im Hellfeld sowie die Darstellung des aktuellen Stands der empirischen Forschung zu den Opfern und Tätern an.

Begriffsdefinition

Im Allgemeinen werden unter Cybercrime oder auch Internetkriminalität Taten verstanden, die mittels der Nutzung des Internets begangen werden. Eine einheitliche Definition liegt allerdings nicht vor (Huber 2019, S. 22 ff.). Es wird zwischen Cybercrime im engeren Sinn (CCieS) („core cybercrime“ bzw. „cyber-dependent crime“), also Delikten, die es nicht offline gibt, wie z. B. Hacking, und Cybercrime im weiteren Sinn (CCiwS) („noncyber-specific cybercrime“ bzw. „cyber-enabled crime“) unterschieden. Letzteres umfasst Delikte, die ebenso offline begangen werden können, wie Kreditkartenmissbrauch. Außerdem werden unter diesen Deliktsbereich Taten zusammengefasst, bei denen gestohlene Identitäten zum Einsatz kommen. Ferner scheint je nach Kontext eine Differenzierung nach Art der Attacke sinnvoll. Es existieren hierbei zielgerichtete und ungerichtete Attacken. Letztere werden auch als „opportunistisch“ beschrieben, da sie sich gegen kein bestimmtes Ziel richten, aber beispielsweise in Form von Schadprogrammen, die das Internet nach Schwachstellen absuchen, Nutzer schädigen (Huber 2019, S. 26 f.). Andererseits haben räuberische bzw. marktorientierte Angriffe in erster Linie das Ziel, Daten zu stehlen und die gestohlenen Inhalte und Daten weiterzuverkaufen.

Computerbetrug wird durch § 263a StGB unter Strafe gestellt. Bestraft wird nach dieser Vorschrift, „wer in der Absicht, sich oder einem Dritten einen rechtswidrigen Vermögensvorteil zu verschaffen, das Vermögen eines anderen dadurch beschädigt, dass er das Ergebnis 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 beeinflusst [...]“.

Unter Cyberkriminalität bzw. CCieS werden in der *Polizeilichen Kriminalstatistik (PKS)* seit 01.01.2016 folgende Arten des Computerbetrugs nach § 263a StGB aufgeschlüsselt: betrügerisches Erlangen von Kraftfahrzeugen, weitere Arten des Kreditbetrugs, Betrug mittels rechtswidrig erlangter Daten von Zahlungskarten, Betrug mittels rechtswidrig erlangter sonstiger unbarer Zahlungsmittel, Leistungskreditbetrug, Abrechnungsbetrug im Gesundheitswesen und Überweisungsbetrug (BKA 2020d, S. 22 f.). Auch sonstiger Computerbetrug wird hierunter gefasst (§ 263a Abs. 1 und 2 StGB sowie Vorbereitungshandlungen gemäß § 263a Abs. 3 StGB). Außerdem werden das Ausspähen und Abfangen von Daten und die Datenhehlerei (§§ 202a, 202b, 202c, 202d StGB), die Fälschung beweiserheblicher Daten und die Täuschung im Rechtsverkehr bei Datenverarbeitung (§§ 269, 270 StGB), die Datenveränderung bzw. die Computersabotage (§§ 303a, 303b StGB) und die missbräuchliche Nutzung von Telekommunikationsdiensten (§ 265a StGB) darunter verstanden. In der *PKS* werden außerdem Taten aufgeführt, bei denen das Internet lediglich als Tatmittel fungiert (BKA 2019a, S. 2 f.).

Verbreitung von Internetkriminalität im Hellfeld (Überblick)

Das Bundeskriminalamt (BKA) veröffentlicht jährlich einen Lagebericht zu Cybercrime, in dem die aktuellen Entwicklungen dargestellt werden. Die Grundlage des Bundeslagebilds Cybercrime sind die Hellfelddaten der *PKS* und nichtpolizeiliche Daten aus dem Dunkelfeld, u. a. von Forschungseinrichtungen oder Behörden, wie dem Bundesamt für Sicherheit in der Informationstechnik (BSI) (BKA 2019a, S. 2).

Das Bundeslagebild bezieht sich in erster Linie auf CCieS-Daten, es werden jedoch auch Ereignisse dargestellt, bei denen Informations- und Kommunikationstechnik zu Planung, Vorbereitung oder Ausführung einer sonstigen Tat benutzt wurde (CCiWS). Bei der Interpretation der *PKS*-Daten verweisen die Autoren darauf, dass z. B. Ransomwaredelikte, bei denen Schadsoftware dazu dienen soll, Lösegeld zu erpressen, in der *PKS* in der Regel nicht als Cybercrimedelikt, sondern als Erpressungsdelikt erfasst werden (BKA 2019a, S. 4 f.). Ferner geht das BKA davon aus, dass eine hohe Dunkelziffer besteht, und dass sich viele Opfer nicht bewusst sind, von Cyberkriminalität betroffen zu sein, z. B. weil sie einen Datendiebstahl nicht bemerkt haben (BKA 2019a, S. 48).

Im Jahr 2019 wurden in der *PKS* insgesamt 100.514 Fälle aus dem Bereich CCieS erfasst, was einer Zunahme der Fallzahlen zum Vorjahr von 15,4 % entspricht (2018:

87.106) (BKA 2020b). Von 2017 bis 2018 wurde lediglich eine Steigerung der polizeilich erfassten Fälle um 1,3 % registriert (2017: 85.960). Die Aufklärungsquote betrug im Jahr 2019 32,3 %.

Seit 2004 wird die *PKS* um die Sondererkennung „Tatmittel Internet“ ergänzt. Eine bundesweite Umsetzung der Zählung wurde 2010 erreicht, weshalb ein Vergleich auf Bundesebene erst ab diesem Jahr möglich ist (BKA 2019b, S. 33). Während im Berichtsjahr 2018 271.864 Fälle mit dem Tatmittel Internet polizeilich erfasst wurden, erhöhte sich die registrierte Fallzahl dieser Straftaten im Jahr 2019 auf 294.665 (BKA 2020c). Dies entspricht einer Steigerung um 8,4 %. 2019 betrug der Anteil der Delikte mit dem Tatmittel Internet an den in der *PKS* registrierten Straftaten insgesamt 5,4 %.

Erscheinungsformen der Cyberkriminalität

Identitätsdiebstahl und Malware

Die Erscheinungsformen von Cybercrime sind vielfältig. Der Phänomenbereich kann nach Art des Delikts oder der Begehungsmethode abgegrenzt werden. Oftmals ist der Ausgangspunkt weiterer krimineller Aktivitäten im Internet der digitale Identitätsdiebstahl (BKA 2019a, S. 1). Unter dem Begriff der „digitalen Identität“ werden zahlreiche personenbezogene Daten zusammengefasst wie z. B. Kommunikationsdaten (E-Mail, Messengerdaten) oder Bankdaten (E-Commerce, Onlineaktienhandel) bis hin zu berufsspezifischen Informationen (Zugriff auf firmeninterne Informationen) (BKA 2019a, S. 12). Hierbei existieren zahlreiche Methoden, um die Daten Betroffener zu stehlen, beispielsweise durch Phishing („nach Passwörtern angeln“) (Huber 2019, S. 101 ff.). Der Diebstahl digitaler Identitäten kann für die Täter verschiedene Zwecke erfüllen, z. B. können die Daten an Dritte weiterverkauft werden, oder die Täter benutzen die gestohlenen Daten selbst für die Bereicherung des eigenen Vermögens (Ziercke 2013, S. 313 f.). Eine besondere Bedeutung kommt hierbei dem Phishing im Zusammenhang mit Onlinebanking zu, auch wenn das Phänomen derzeit einem rückläufigen Trend unterliegt (Huber 2019, S. 17). Ferner werden vermehrt Taten registriert, bei denen, wie beim „Doxing“, Daten entwendet werden, mit denen versucht wird, dem Ansehen von Personen etwa durch die Veröffentlichung intimer Daten zu schaden (Huber 2019, S. 15 ff.).

Der Identitätsdiebstahl wird oftmals durch sog. Malware gesteuert (Huber 2019, S. 111). Unter dem Phänomen Malware, deutsch Schadsoftware, sind verschiedene Arten von schädlichen Attacken zusammengefasst, wie etwa Viren, Trojaner, Spyware oder Würmer. Durch das Einschleusen von Schadsoftware übernehmen Hacker ohne Kennt-

nis des Benutzers die Steuerung des Computers. Schadsoftware kann hierbei über sog. Botnetzprogramme gesteuert werden. Unter Botnetzen versteht man ein Netzwerk ferngesteuerter Computer, die ohne Wissen der Besitzer über einen Schadcode infiziert wurden, um z.B. die persönlichen Daten des Besitzer an die Täter weiterzuleiten (Ziercke 2013, S. 318f.).

Außerdem kann Schadsoftware beispielsweise beim Phishing eingesetzt werden, also dem Versuch, über gefälschte Webseiten, versendete E-Mails oder Chats an Nutzerdaten zu gelangen (Huber 2019, S. 80ff.). Während im privaten Bereich v.a. der Diebstahl von Zugangs- oder Bezahltdaten Schaden für die Nutzer birgt, kann Schadsoftware im wirtschaftlichen Bereich die Existenz von Unternehmen bedrohen (Huber 2019, S. 76f.). Es wird ständig neue Schadsoftware entwickelt. Das Gesamtaufkommen von Malware belief sich 2018 nach Angaben des BKA, unter Rückgriff der Daten des BSI und des Sicherheitsunternehmens AV-Test, auf über 800 Mio. Varianten (BKA 2019a, S. 19).

Die Bandbreite der Anwendung von schädlichen Programmen zeigen digitale Angriffe auf Geldautomaten unter Rückgriff auf Schadsoftware, die in jüngster Zeit an Bedeutung zunehmen, auch wenn die Fallzahlen (noch) relativ gering ausfallen (BKA 2019a, S. 22). Hierbei können unterschiedliche Methoden angewandt werden, die zum „cash-out“ führen sollen, in dem z.B. ein Malwareangriff auf die kartenausgebende Bank gestartet wird, um Transaktionsprozesse zu manipulieren. Im Jahr 2018 wurden beispielsweise drei asiatische Banken durch derartige Netzwerkattacken angegriffen, was einen Cash-out in Deutschland und anderen Ländern zur Folge hatte und nach Angaben des Bundeslageberichts zu einem weltweiten Schaden von ca. 39 Mio. Euro geführt haben soll. Netzwerkattacken auf Geldautomaten werden seit dem Jahr 2016 weltweit vermehrt mit Schadenssummen im mehrfachen Millionenbereich verzeichnet (BKA 2019a, S. 23).

Außerdem gewinnt der Einsatz von Ransomware im Zusammenhang mit Schadprogrammen an Bedeutung. Bei Ransomware (Lösegeld, engl. „ransom“) handelt es sich um eine Kombination der Delikte Computersabotage gemäß § 303b StGB und Erpressung gemäß § 253 StGB (BKA 2019a, S. 25). Hierbei werden durch das Verbreiten einer Schadsoftware z.B. Daten eines digitalen Systems verschlüsselt oder Endgeräte in Firmennetzwerken gesperrt und somit ganze Netzwerke gestört, was zu einem kompletten Ausfall des Geschäftsbetriebs führen kann. Meist fordern die Täter ein Lösegeld, was die Betroffenen in Form von Kryptowährungen (digitale Währungen) zahlen sollen, um einen Freischaltcode zur Entsperrung des Systems zu erhalten. Oftmals zahlen die Geschädigten das in Relation zum potenziellen Schaden geringe Lösegeld aus Angst vor weitreichenden Folgen für das System (BKA

2019a, S. 24ff.). Die Polizei rät von den Zahlungen zur Entsperrung ab, da hierdurch ein Anreiz für die Täter geschaffen wird.

Ein aktuelles Beispiel für Schadsoftware aus dem Bundeslagebericht 2018 ist die Verbreitung von Botnetzwerken (BKA 2019a, S. 28). Das BSI gab für das Jahr 2018 an, 10.000 Botnetzinfektionen deutscher Systeme registriert zu haben (BKA 2019a, S. 29). Botnetze werden beispielsweise für DDoS-Angriffe genutzt (BKA 2019a, S. 28ff.). Bei DDoS-Angriffen („distributed denial of service“) werden umfangreiche Datenanfragen an Server gestellt, die zum Zusammenbrechen der Systeme führen (BKA 2019a, S. 31). Seit 2018 werden vermehrt Clouds (wie z.B. die Amazon Cloud) als Adressaten dieser Angriffe registriert, um die Plattform anzugreifen oder über die infizierte Plattform Cyberangriffe zu starten. Es erfolgte ein Zuwachs an Angriffen von 80 % durch DDoS-Angriffe über widerrechtlich genutzte Cloud-Server zum Jahr 2017 (BKA 2019a, S. 31). Aber auch der Zahlungsdienstleister Pay-Pal und der Energieerzeuger RWE waren 2018 Ziel dieser Attacken (BKA 2019a, S. 32ff.). Die Motivation für diese Art von Angriffen erstreckt sich über monetäre Interessen bis hin zu politischen Beweggründen. Malware wird immer häufiger auf mobilen Endgeräten zum Problem, um beispielsweise an Bankdaten zu gelangen oder sich Eintritt in Firmennetzwerke zu schaffen (BKA 2019a, S. 34).

Digitale Schwarzmärkte

Für die Verbreitung kinderpornografischen Materials sowie für andere Straftaten wie den Handel mit Betäubungsmitteln, Waffen oder Falschgeld nutzen Täter oftmals spezifische Plattformen (BKA 2019a, S. 38ff.). Im Gegensatz zu dem frei zugänglichen Open Web (Clearnet) wird hierfür das Deep Web (Hidden Web, Invisible Web) oder das Darknet genutzt. Während das Deep Web zwar nicht durch Suchmaschinen auffindbar ist, aber mit geläufigen Internetbrowsern erreicht werden kann, ist der Zugang zum Darknet nur durch die Nutzung einer speziellen Software möglich. Allein im Jahr 2017 wurden 6 solcher Plattformen durch die Strafverfolgungsbehörden abgeschaltet. Beispielsweise wurde durch die im Juli 2017 ausgeschaltete Plattform AlphaBay, auf der Drogen, Waffen und Betrugsgüter gehandelt wurden, bei einer Laufzeit von zweieinhalb Jahren ein Gewinn von ca. 628 Mio. € generiert (BKA 2019a, S. 41). Drescher (2019) schätzte im Rahmen seiner Literaturanalyse zu Industrie- und Wirtschaftsspionage in Deutschland den jährlichen wirtschaftlichen Schaden für die Bundesrepublik auf ca. 12 Mrd. € (Drescher 2019, S. 90f.).

Außerdem werden auf digitalen Marktplätzen cyberkriminelle Dienstleistungen angeboten. „Cybercrime-as-a-Service“ umfasst u.a. die Herstellung von Malware, den digitalen Datendiebstahl oder Dienste zur Verschleierung der

Identität. Zudem werden Unterstützungsleistungen angeboten, wie etwa Updates von Malware (BKA 2019a, S. 42). Digitale Währungen wie Bitcoin sind hierbei ein beliebtes Zahlungsmittel. Der illegale Erwerb von Kryptowährungen (digitale Zahlungsmittel) stellt ebenfalls ein Ziel von Tätern dar. Die digitale Geldwäsche ist ein wachsendes Phänomen, was durch die fehlende Umsetzung von Antigeldwäschegesetzen im Internet befördert wird (BKA 2019a, S. 43).

Ferner verweist das BKA in seinem Lagebericht darauf, dass sich „Living-off-the-Land“ („LotL“-Methoden und „supply chain attacks“ stark verbreiten. Bei der „LotL“-Methode wird Datendiebstahl oder die Verbreitung von Malware durch die Zweckentfremdung einer Software oder eines Tools durchgeführt, ohne dass Malware installiert wird. Supply chain attacks infizieren über Schwachstellen in Systemen (Supply chain) zunächst Teilsysteme oder Informationsketten über Dritte, bevor die eigentliche Cyberattacke erfolgt (BKA 2019a, S. 44).

Außerdem sieht das BKA das „Internet der Dinge“ oder auch „internet of things“ (Iot) als einen Angriffspunkt, der in Zukunft verstärkt von Tätern für den Datendiebstahl genutzt werden wird (BKA 2019a, S. 45 f.). Dieser Begriff bezeichnet die Vernetzung von Gegenständen mit dem Internet (u. a. Smartphones, Sprachassistenten oder Sicherheitskameras) (Jararweh et al. 2015, S. 453). Inzwischen verfügt nach Angaben des Bundeslageberichts jeder Haushalt durchschnittlich über 6 Iot-Geräte (BKA 2019a, S. 45). Der *McAfee Labs Threats Report* identifizierte allein im 3. Quartal 2018 ca. 45.000 neu aufgekommene Malware, die auf Iot-Geräte spezifiziert war (McAfee 2018, S. 28).

Der BKA-Lagebericht verweist neben Angriffen auf Privatpersonen und Unternehmen auf Gefahrenpotenziale durch Cyberangriffe auf die sog. kritischen Infrastrukturen (KRITIS). Diese umfassen verschiedene Sektoren, wie Energie, Wasser, Ernährung, Kommunikationstechniken, Gesundheit, Medizin, Staat und Verwaltung (BKA 2019a, S. 47). Das BSI wies im Zeitraum vom 01.06.2017 bis 31.05.2018 insgesamt 145 meldepflichte Störungen aus; der Schwerpunkt lag im Bereich Informationstechnik und Telekommunikation (Bundesamt für Sicherheit in der Informationstechnik [BSI] 2018, S. 10).

Eine weitere Herausforderung von Cybercrime im weiteren Sinne stellt Betrug mittels „technical support scams“ dar. Hierbei geben sich Täter am Telefon als Mitarbeiter einer Softwarefirma aus und weisen ihre Opfer an, bestimmte Tools zu installieren, um ein vermeintliches Problem zu lösen. Letztendlich wird eine gefälschte Zahlungsaufforderung generiert (BKA 2019a, S. 43).

Sexualbezogene Tatbestände

Weiter werden im Phänomenbereich Cybercrime sexualbezogene Straftaten begangen. Unter dem Begriff der

Kinderpornografie wird illegales pornografisches Material mit Abbildungen echter Personen mit kindlichem Erscheinungsbild erfasst, die an sexuellen Handlungen beteiligt sind (Franke und Graf 2016, S. 88). Kinderpornografische Medien können verschiedene Erscheinungsformen umfassen, die auf der sog. COPINE-Skala, einem System zur Klassifizierung der Schwere von Darstellungen des sexuellen Kindesmissbrauchs, eingeordnet werden und von nichtsexuellen Bildern, z. B. Fotos von Kindern in Unterwäsche, bis hin zu sadistischen und zoophilen Handlungen reichen. Die Strafverfolgung wird insbesondere durch die Herstellung, den Konsum und die Verbreitung im internationalen Raum erschwert. Die Organisation pädophiler Täter wird durch die Produktion, Verteilung und den Konsum von Kinderpornografie über das Internet, die Kontaktabnähung mit potenziellen Opfern zur Vorbereitung von Übergriffen („cyber-grooming“) sowie die Bildung von subkulturellen Täternetzwerken im Internet begünstigt (Franke und Graf 2016, S. 90). Beim Tatbestand des Cyber-grooming täuschen Erwachsene oftmals eine falsche Identität vor, um ihre Opfer u. a. dazu zu nötigen, ihnen sexuelle Fotos oder Videos zu schicken (Huber 2019, S. 146). Die *Internet Watch Foundation* (IWF), die es sich zum Ziel macht, die Verfügbarkeit von Onlineinhalten für sexuellen Missbrauch zu reduzieren, hat allein im Jahr 2018 über 105.047 Seiten mit kinderpornografischen Inhalten aufgefunden. Im Vorjahr waren es 78.589 (Internet Watch Foundation [IWF] 2018). Die hohe Summe an gefundenen Webseiten ist auch auf verbesserte technische Möglichkeiten, entsprechende Medien zu erkennen, zurückzuführen (Internet Watch Foundation [IWF] 2019).

Beim Cyberstalking wird in erster Linie das Internet für beharrliche Nachstellungen und Bedrohungen bzw. Belästigungen genutzt (Huber 2019, S. 132). Dabei ist Stalking unter der Verwendung von Telekommunikationsmitteln, sonstigen Mitteln der Kommunikation oder über Dritte in § 238 StGB als Unterfall der Nachstellung aufgeführt. Huber (2019) beschreibt darüber hinaus eine Mischform zwischen Identitätsdiebstahl und Cyberstalking, bei der sich Täter das Profil (u. a. das Social-Media-Profil) ihres Opfers aneignen und in dessen Namen Bilder oder Texte veröffentlichen (Huber 2019, S. 111). Das „sextortion“ stellt eine Art von Erpressung dar, bei dem der Täter vorgibt, das Opfer z. B. beim Masturbieren gefilmt zu haben, und diesem mit der Veröffentlichung des Materials droht (BKA 2019a, S. 44).

Künftige Erscheinungsformen

Der fortschreitende Einsatz von Computersystemen im Alltag wird weitere Möglichkeiten für Cyberangriffe bieten (Honekamp 2019, S. 54). Smart Homes, Cloud Computing und Big Data sind nur beispielhaft genannte Entwicklungen

in einer zunehmend digitalisierten Welt, mit denen großes Potenzial für einen Missbrauch digitaler Daten verbunden ist. Außerdem ist an dieser Stelle die problematische Verbreitung von unrichtigen Nachrichten (Fake News) zu nennen, bei der es zur Begehung von Straftaten kommen kann. Es ist davon auszugehen, dass Identitätsdiebstahl weiterzunehmen wird, ebenso die Nutzung des Darknet als illegale Verkaufsplattformen. Honekamp prognostiziert, dass die zukünftigen Angriffsziele mobile Systeme von Endgeräten sein werden (Honekamp 2019, S. 55). Der nahezu dauerhafte Anschluss an das Internet befördert cyberkriminelle Straftaten, da hierdurch dem Angreifer eine größere Aussicht auf Erfolg durch vielfältige Tatgelegenheiten gegeben wird.

Die digitale Transformation manifestiert sich zudem in der digitalen Produktion. Dieser Wandel wird mit dem Begriff Industrie 4.0 beschrieben (Eckert 2017, S. 141). Das Verschwinden von digitalen und physikalischen Grenzen, wie z. B. beim automatisierten Fahren oder bei der vernetzten Gesundheitsversorgung, birgt zunehmend Risiken für Unternehmen und stellt die IT-Sicherheit-Forschung vor immer neue Herausforderungen (Eckert 2017, S. 146). Bezogen auf alle Arten von cyberkriminellen Straftaten bewertet das BSI den Einsatz von Ransomware als die größte Bedrohung für Unternehmen, Behörden, sonstige Institutionen und Privatanwender (das Bundesamt für Sicherheit in der Informationstechnik [BSI] 2019, S. 75). Komplettausfälle von Computern und Netzwerken sowie von Produktionsanlagen stellen weitreichende Folgen eines Ransomwareangriffs dar. Die Kosten für die betroffene Institution sind u. a. aufgrund von Produktionsausfällen, Datenverlust und Wiederherstellung von Systemen enorm.

Opfer

Im Jahr 2019 führte das BSI gemeinsam mit der *Polizeilichen Kriminalprävention der Länder und des Bundes* (ProPK) eine Bürgerbefragung zur Cybersicherheit durch (Bundesamt für Sicherheit in der Informationstechnik [BSI] und Polizeiliche Kriminalprävention der Länder und des Bundes [ProPK] 2019). Hierzu wurde eine Stichprobe aus der deutschen Bevölkerung im Alter von 16 bis 69 Jahren gezogen, und die Studienteilnehmer wurden mithilfe einer Onlinebefragung interviewt (BSI und ProPK 2019, S. 3). Es wurden 2000 Interviews geführt und die Studienteilnehmer nach dem Onlinenutzungsverhalten und dem Sicherheitsempfinden, zum Informationsverhalten zur IT-Sicherheit, zur Bekanntheit und zum Nutzen des BSI und der ProPK sowie zur Viktimisierungserfahrung mit Cyberkriminalität befragt. Die Umfrage Digitalbarometer ergab, dass 24 % der Befragten bereits Opfer von Internetkriminalität wurden (BSI und ProPK 2019, S. 4). Von den Studienteilneh-

mern verneinten 69 % eine entsprechende Opfererfahrung (BSI und ProPK 2019, S. 6). Die Mehrheit der Betroffenen gab an, Opfer von Betrugsdelikten beim Onlineshopping geworden zu sein (36 %), gefolgt von Phishingvorfällen (28 %) und Angriffen durch eine Schadsoftware mittels Viren oder Trojanern (26 %). Von einem Identitätsdiebstahl berichteten 18 % der Betroffenen. Etwas geringer war der Anteil derer, die durch Ransomware erpresst wurden (13 %) oder von Cybermobbing betroffen waren (13 %). Von den Studienteilnehmern schätzten 24 % die Gefahr, Opfer von Cyberkriminalität zu werden, als hoch ein, 5 % der Befragten bewerteten die Gefahr als sehr hoch (BSI und ProPK 2019, S. 6).

Lediglich 61 % der Befragten schützten sich durch Antivirenprogramme gegen Cyberangriffe, und 58 % der Befragten gaben an, sichere Passwörter zu benutzen (BSI und ProPK 2019, S. 5). Eine sofortige Installation von Updates führten 36 % der Befragten durch, und auf die Möglichkeit zur E-Mail-Verschlüsselung griffen 19 % zurück.

Das BKA erhob im Rahmen des *Deutschen Viktimisierungssurvey 2017* (DVS 2017) die Opferbelastung durch Internetkriminalität. Neben anderen Straftaten, wie z. B. Diebstahl, Raub und Körperverletzung, wurde die Viktimisierungserfahrung zu Cyberkriminalität u. a. in einem Fünfjahresprävalenzzeitraum untersucht (BKA 2019c). Die Personen wurden telefonisch befragt, ob sie Opfer einer Schadsoftware wurden, zur Preisgabe von sensiblen Daten (z. B. Passwörter) durch betrügerische E-Mails (Phishing) oder zur Preisgabe solcher Daten durch die Umleitung auf gefälschte Internetseiten verleitet wurden (Pharming). Im Vergleich zu dem im Jahr 2012 durchgeführten DVS zeigte sich im Hinblick auf Datenverlust oder sonstige Schäden, die durch eine Schadsoftware verursacht wurden, ein Rückgang in der 2017 beobachteten Prävalenzrate (BKA 2019c, S. 16). Während 2012 von 35.503 befragten Personen 24,1 % angaben, von einem entsprechenden Delikt betroffen gewesen zu sein, bejahten 19,1 % der 31.192 Befragten des Surveys 2017 die Opfererfahrung. Ungeachtet des Rückgangs ist sowohl 2012 als auch 2017 die Schädigung durch eine Schadsoftware das am häufigsten berichtete Delikt. Ein Anstieg der Prävalenzrate wurde bei den Internetdelikten Phishing und Pharming beobachtet. Während 2012 2,4 % der Befragten angaben, zur Preisgabe sensibler Daten durch betrügerische E-Mails verleitet worden zu sein, waren es 2017 3,1 % der Befragten. Der Anteil der von Pharming Betroffenen lag 2012 bei 1,4 % und 2017 bei 2,0 %.

Nicht selten sind neben Privatpersonen auch Unternehmen von Cyberangriffen bedroht (Honekamp 2019, S. 48). Der Digitalverband *Bitkom* untersuchte in einer Studie 2018 die Betroffenheit der deutschen Industrie von Spionage, Sabotage und Datendiebstahl (Bitkom e. V. 2019). Hierzu wurden 503 Führungskräfte aus repräsentativ ausgewählten In-

dustrieunternehmen telefonisch befragt (Bitkom e. V. 2019, S. 6). Die Studie ergab, dass 68,8 % der Unternehmen in den letzten 2 Jahren von Datendiebstahl, Industriespionage oder Sabotage betroffen waren. Weitere 19,0 % der befragten Unternehmen gaben an, vermutlich von einem Cyberangriff betroffen gewesen zu sein (Bitkom e. V. 2019, S. 14). Mit 73,0 % waren am stärksten Industrieunternehmen gefährdet, die über eine Unternehmensgröße von 100 bis 499 Mitarbeitern verfügten. Geschuldet kann dies der Tatsache sein, dass insbesondere der Mittelstand in Deutschland als besonders innovativ gilt und eine starke Einbindung in die Lieferketten von Großkonzernen aufweist. Es besteht daher die Vermutung, dass die Angreifer hauptsächlich an dem Spezialwissen kleinerer Unternehmen interessiert sind und zudem kleinere Unternehmen dazu nutzen, die Daten von großen Konzernen abzufangen. Die geringste Betroffenheit wurde bei den Unternehmen mit der größten Mitarbeiteranzahl (ab 500 Mitarbeiter) festgestellt. Dies kann auf den Einsatz eines besseren Schutzes von Großkonzernen zurückzuführen sein (Bitkom e. V. 2019, S. 14).

Der Diebstahl von IT- oder Telekommunikationsgeräten war nach der Befragung 2018 mit 32 % der häufigste Vorfall, gefolgt von Diebstahl von sensiblen digitalen Daten bzw. Informationen (23 %) (Bitkom e. V. 2019, S. 15f.). Deutlich seltener fand eine Offlinesabotage von Informations- und Produktionssystemen oder Betriebsabläufen statt (10 %) und/oder wurden Besprechungen oder Telefonate abgehört (9 %). Bei dem Datendiebstahl handelte es sich vorrangig um unkritische Geschäftsinformationen (67 %), gefolgt von Kommunikationsdaten, wie z. B. E-Mails (48 %) und Kundendaten (21 %). Von den Befragten gaben 20 % an, Opfer von Finanzdatendiebstahl geworden zu sein.

Mehrheitlich traten in den letzten zwei Jahren in Chemie- und Pharmaunternehmen (74 %) und in Unternehmen des Automobilbaus (68 %) Datendiebstähle, Industriespionage oder Sabotage auf (Bitkom e. V. 2019, S. 17). Etwas geringer war die Betroffenheit von Unternehmen im Maschinen- und Anlagenbau (67 %) und Industrieunternehmen zur Herstellung von Kommunikations- und Elektrotechnik (63 %).

Die Annahme, eine zunehmende Digitalisierung im Unternehmen stehe im Zusammenhang mit steigenden Sicherheitsrisiken, wurde durch die Studie nicht bestätigt (Bitkom e. V. 2019, S. 18). Die Befragung kam zu dem Ergebnis, dass Unternehmen mit einem niedrigen Digitalisierungsniveau mit 71 % häufiger von Cyberkriminalität betroffen waren als Unternehmen, die über ein hohes Digitalisierungsniveau verfügten (64 %).

Vorrangig führte ein Hinweis durch eine unternehmensinterne Person zur Aufdeckung des Vorfalls (61 %) (Bitkom e. V. 2019, S. 30). Das eigene Sicherheitssystem, Virens Scanner und/oder Firewall lieferten in 40 % der Fälle Hinweise auf einen Angriff, und durch eine interne Revisi-

on bzw. interne Ermittlungseinheit wurden 38 % der Fälle bekannt. Nur 3 % der Cyberdelikte wurden aufgrund von Hinweisen durch Strafverfolgungs- bzw. Aufsichtsbehörden aufgedeckt.

Einen Überblick über die empirische Studienlage zu Cybercrime gegen Organisationen auf der Grundlage ausländischer Viktimisierungsuntersuchungen haben *Köllisch und Jähnke* (2006) erstellt. Die Autoren schlossen 9 Studien der Jahre 1996–2005 in die Übersichtsarbeit ein, um die Prävalenzraten und den Schadensumfang von cyberkriminellen Angriffen gegen Organisationen in Europa, Australien und den USA zu ermitteln (Köllisch und Jähnke 2006, S. 366 ff.). Es bestanden Unterschiede zwischen den länderspezifischen Viktimisierungsprävalenzen, jedoch wurden die Schwankungen auf die unterschiedliche Stichprobenzusammensetzung der einzelnen Studien zurückgeführt (Köllisch und Jähnke 2006, S. 385). Die Autoren führten an, dass das Vorkommen von Cyberkriminalität gegen Organisationen zumindest in den Industrienationen eine ubiquitäre Verteilung aufweist. Der Vergleich der Studien zeigte, dass Organisationen am häufigsten von Viren, Würmern und Trojanern betroffen waren (Köllisch und Jähnke 2006, S. 376). In den meisten Studien wird am zweithäufigsten von einem Missbrauch von IT-Ressourcen durch einen Mitarbeiter der Organisation berichtet, gefolgt vom Ausspähen von Daten durch einen Hackerangriff. Gemäß den Studienergebnissen entstanden die größten Schäden für die Organisation durch Betrugsdelikte und Informationsdiebstahl (Köllisch und Jähnke 2006, S. 381). Angaben zu der Reaktion auf die entdeckten Cyberangriffe waren den Studien laut *Köllisch und Jähnke* nur vereinzelt zu entnehmen. Anzeige wurde in weniger als einem Fünftel der Fälle erstattet (Köllisch und Jähnke 2006, S. 382 ff.).

Täter

Im Jahr 2019 wurden in der PKS 22.574 Tatverdächtige im Deliktbereich CCieS registriert. Der Großteil der Tatverdächtigen war mit 68,3 % männlich ($n = 15.423$) (BKA 2020f). Es waren 31,7 % der Tatverdächtigen weiblich ($n = 7151$). Aus dem Bundeslagebild 2018 geht hervor, dass im Hinblick auf die CCieS-Straftaten weibliche Tatverdächtige im Verhältnis zu den Straftaten insgesamt (24,9 %) überrepräsentiert waren (BKA 2019a, S. 7). Dies resultierte vornehmlich aus dem Straftatbestand des Computerbetrugs, der hohe Fallzahlen und gleichzeitig einen hohen Anteil an weiblichen Tatverdächtigen aufweist. Zu 75,4 % hatten die Tatverdächtigen 2019 die deutsche Staatsangehörigkeit (BKA 2020a). Unter den nichtdeutschen Tatverdächtigen bildeten türkische (13,2 %), rumänische (9,2 %) und polnische (6,1 %) Staatsangehörige die größte Gruppe (BKA 2020e). In der PKS 2019 wurden mehrheitlich junge Er-

wachsene als tatverdächtige Personen registriert. Von den Tatverdächtigen waren 57,4 % in einem Alter von 21 bis 39 Jahren (BKA 2020a). Gemäß dem Bundeslagebild 2018 agierten die Tatverdächtigen sowohl allein als auch in organisierten Tätergruppen. Zudem wies das Bundeslagebild 2018 154.773 Fälle mit Waren- und Warenkreditbetrug aus, bei denen Täter ihre über das Internet angebotenen Waren nicht oder in minderwertiger Qualität lieferten oder Tatverdächtige Waren bestellten, aber nicht bezahlten (BKA 2019a, S. 8 ff.).

Eine Untersuchung des *United Nations Office on Drugs and Crime* (UNODC) zu Cybercrime verwies auf den bestehenden Mangel an evidenzbasierten Studien zu Cyberkriminalität (UNODC 2013, S. 39). Es mangle insbesondere am Wissen über die Täter, die Delikte im Bereich der Kinderpornografie im Online- und im Offlinestatus begehen. Die täterbezogenen Angaben, die im Bericht des UNODC beschrieben werden, stützen sich auf die Auswertung von 4 einschlägigen Studien. Die Studien stimmten hinsichtlich des Alters und des Geschlechts der Täter von Cyberkriminalität weitestgehend überein. Es handelte sich bei der Mehrheit der Täter um junge Erwachsene zwischen 18 und 30 Jahren, die vorrangig männlichen Geschlechts waren (UNODC 2013, S. 41 f.). Aufgrund der sofortigen Verfügbarkeit von Malware-Toolkits sind komplexe Fähigkeiten oder Techniken laut UNODC nicht zwingend erforderlich, um Cybercrimedelikte zu begehen (UNODC 2013, S. 42).

Huber und Pospisil (2018) führten eine Aktenanalyse durch und erhoben u. a. Merkmale der Tatverdächtigen, die wegen eines Internetdelikts angeklagt wurden. Gegenstand der Untersuchung waren 89 Fallakten zu Cybercrimedelikten des Wiener Straflandesgerichts, denen Angaben zu 118 Tatverdächtigen entnommen wurden (Huber und Pospisil 2018, S. 21 ff.). Der Untersuchungszeitraum erstreckte sich über die Jahre 2006–2016. Die Studie ergab, dass die Tatverdächtigen im Bereich cyberkrimineller Straftaten mehrheitlich männlich (83,2 %) und vorrangig zwischen 21 und 30 Jahre alt waren (40 %) (Huber und Pospisil 2018, S. 23 f.). Ferner wies die Mehrheit der Tatverdächtigen ein geringes Bildungsniveau auf (73,6 %) und ging zum Zeitpunkt der Tat keiner Beschäftigung nach (61 %). Die deutliche Mehrheit war nicht im IT-Bereich tätig (94,1 %). Ein Drittel der Tatverdächtigen war bereits strafrechtlich in Erscheinung getreten (Huber und Pospisil 2018, S. 36). Die Studienergebnisse deuten auf einen Zusammenhang zwischen der Komplexität der Delikte und dem Bildungsniveau des Täters hin. Vorrangig werden komplexe Cyberattacken von Personen begangen, die über höhere IT-Sicherheits- bzw. Informationskenntnisse verfügen, im Vergleich zu Personen, die weniger aufwendige und weniger detailliert geplante cyberkriminelle Angriffe verüben (Huber und Pospisil 2018, S. 32).

Die im vorangegangenen Abschnitt zu den Opfern cyberkrimineller Angriffe vorgestellte Studie des Digitalverbands *Bitkom* ging neben der Betroffenheit der deutschen Industrie von Spionage, Sabotage und Datendiebstahl auch der Frage nach der Täterschaft nach (Bitkom e.V. 2019, S. 28 ff.). Am häufigsten wurden ehemalige Mitarbeiter als Täter von Cybercrimedelikten gegen Industrieunternehmen genannt (61 %). Geringer war der Anteil von Privatpersonen bzw. Hobbyhackern (29 %), konkurrierenden Unternehmen (22 %) und organisierten Banden (17 %). In 15 % der Fälle waren Kunden die Täter. Externe Dienstleister bzw. Berater wurden in 9 % der Fälle als Täter benannt und eigene derzeitige Mitarbeiter in 7 % der Internetdelikte. In 4 % der Fälle war der Täter nicht bekannt, oder es lagen zu einem Vorfall keine Angaben zum Täter vor.

Steinmetz stellte in einer ethnografischen Studie zu Cyberhacking den Versuch an, ein fundiertes Verständnis zu den Tätern von Cyberangriffen zu entwickeln (Steinmetz 2015). Hierzu wurde ein qualitatives Datenerhebungsverfahren gewählt und die teilnehmende Beobachtung von Mitgliedern der Hackerszene um semistrukturierte Interviews mit Studienteilnehmern ($n=16$) ergänzt (Steinmetz 2015, S. 128). Die Autoren der Studie schreiben dem Hacking Merkmale der Handwerkskunst zu. Die Täter zeichneten sich häufig durch gemeinsame Merkmale, wie z. B. durch eine bestimmte Mentalität, eine Betonung der eigenen Fertigkeiten und eine selbsternannte Berufung zum Hacking aus. Steinmetz identifizierte 5 Eigenschaften, die er der Mentalität der Hacker zuordnete: Die mehrheitlich männlichen Befragten verfügten über eine ausgewiesene Neugierde, Neues zu entdecken, waren problemlösungsorientiert, wiesen eine systematische und technische Denkweise auf und waren kreativ und unkonventionell (Steinmetz 2015, S. 130 f.). Zudem wurde ihnen die Fähigkeit zugeschrieben, welche Steinmetz mit „orientation towards breaking and creating“ beschrieb (Steinmetz 2015, S. 132). Damit soll die Eigenschaft beschrieben werden, etwas Gegebenes zu zerstören, umzustrukturieren und letztendlich neu zu erschaffen. Die technische Qualifikation beruhte primär auf dem Erlernen von Technik und weniger auf Begabung. Außerdem wies der Lernprozess soziale Strukturen des Gruppenlernens auf (Steinmetz 2015, S. 134).

Fazit

Aufgrund des fortschreitenden digitalen Wandels sind in immer kürzeren Abständen neue Entwicklungen im Bereich der digitalen Sicherheit unabdingbar. Die Entwicklung präventiver Maßnahmen kann durch eine regelmäßige Durchführung von Befragungen erreicht werden, um so neue Probleme und Sicherheitsrisiken schnellstmöglich zu erkennen und diesen effektiv entgegenwirken zu können. Es bedarf

einer interdisziplinären Vernetzung von Wissenschaftlern, um dem Phänomen der Cyberkriminalität adäquat begegnen zu können. Die IT-Sicherheit-Forschung wird zunehmend mit der Entwicklung neuer Ansätze und Methoden konfrontiert sein, um den Schutz von cyberphysischen Systemen zu gewährleisten. Die Weiterentwicklung der künstlichen Intelligenz (KI) könnte in Zukunft Chancen steigern, Angriffe durch Internetkriminelle schneller zu erkennen, birgt aber auch Risiken, wenn die Täter diese Technologie für ihre kriminellen Zwecke nutzen.

Funding Open Access funding provided by Projekt DEAL.

Interessenkonflikt B. Horten und M. Gräber geben an, dass kein Interessenkonflikt besteht.

Open Access Dieser Artikel wird unter der Creative Commons Namensnennung 4.0 International Lizenz veröffentlicht, welche die Nutzung, Vervielfältigung, Bearbeitung, Verbreitung und Wiedergabe in jeglichem Medium und Format erlaubt, sofern Sie den/die ursprünglichen Autor(en) und die Quelle ordnungsgemäß nennen, einen Link zur Creative Commons Lizenz beifügen und angeben, ob Änderungen vorgenommen wurden.

Die in diesem Artikel enthaltenen Bilder und sonstiges Drittmaterial unterliegen ebenfalls der genannten Creative Commons Lizenz, sofern sich aus der Abbildungslegende nichts anderes ergibt. Sofern das betreffende Material nicht unter der genannten Creative Commons Lizenz steht und die betreffende Handlung nicht nach gesetzlichen Vorschriften erlaubt ist, ist für die oben aufgeführten Weiterverwendungen des Materials die Einwilligung des jeweiligen Rechteinhabers einzuholen.

Weitere Details zur Lizenz entnehmen Sie bitte der Lizenzinformation auf <http://creativecommons.org/licenses/by/4.0/deed.de>.

Literatur

- Bitkom e.V. (2019) Spionage, Sabotage und Datendiebstahl – Wirtschaftsschutz in der Industrie. Studienbericht 2018. <https://www.bitkom.org/sites/default/files/file/import/181008-Bitkom-Studie-Wirtschaftsschutz-2018-NEU.pdf>. Zugriffen: 17. Apr. 2020
- Bundesamt für Sicherheit in der Informationstechnik (BSI) (2018) Die Lage der IT-Sicherheit in Deutschland 2018. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2018.pdf?__blob=publicationFile&v=6. Zugriffen: 22. Apr. 2020
- Bundesamt für Sicherheit in der Informationstechnik (BSI) (2019) Die Lage der IT-Sicherheit in Deutschland 2019. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2019.pdf?__blob=publicationFile&v=7. Zugriffen: 20. Apr. 2020
- Bundesamt für Sicherheit in der Informationstechnik (BSI), Polizeiliche Kriminalprävention der Länder und des Bundes (ProPK) (2019) Digitalbarometer: Bürgerbefragung zur Cyber-Sicherheit. Kurzbericht zu den Umfrageergebnissen der Polizeilichen Kriminalprävention der Länder und des Bundes (ProPK) und des Bundesamts für Sicherheit in der Informationstechnik (BSI). https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Digitalbarometer/Digitalbarometer-ProPK-BSI_2019.pdf?__blob=publicationFile&v=3. Zugriffen: 20. Apr. 2020
- Bundeskriminalamt (BKA) (Hrsg) (2019a) Cybercrime. Bundeslagebild 2018. Bundeskriminalamt, Wiesbaden
- Bundeskriminalamt (BKA) (Hrsg) (2019b) Fälle, Aufklärung, Schaden. Polizeiliche Kriminalstatistik. Bundesrepublik Deutschland. Jahrbuch 2018, Bd. 1. Bundeskriminalamt, Wiesbaden
- Bundeskriminalamt (BKA) (Hrsg) (2019c) Der Deutsche Viktimisierungssurvey 2017. Opfererfahrungen, kriminalitätsbezogene Einstellungen sowie die Wahrnehmung von Unsicherheit und Kriminalität in Deutschland. V 1.0. Bundeskriminalamt, Wiesbaden
- Bundeskriminalamt (BKA) (Hrsg) (2020a) Polizeiliche Kriminalstatistik 2019. Deutsche Tatverdächtige nach Alter und Geschlecht. Bundeskriminalamt, Wiesbaden
- Bundeskriminalamt (BKA) (Hrsg) (2020b) Polizeiliche Kriminalstatistik 2019. Grundtabelle. Bundeskriminalamt, Wiesbaden
- Bundeskriminalamt (BKA) (Hrsg) (2020c) Polizeiliche Kriminalstatistik 2019. Grundtabelle „Tatmittel Internet“. Bundeskriminalamt, Wiesbaden
- Bundeskriminalamt (BKA) (Hrsg) (2020d) Polizeiliche Kriminalstatistik. Bundesrepublik Deutschland. Straftatenkatalog 2019. Bundeskriminalamt, Wiesbaden
- Bundeskriminalamt (BKA) (Hrsg) (2020e) Polizeiliche Kriminalstatistik 2019. Straftaten und Staatsangehörigkeiten nichtdeutscher Tatverdächtiger. Bundeskriminalamt, Wiesbaden
- Bundeskriminalamt (BKA) (Hrsg) (2020f) Polizeiliche Kriminalstatistik 2019. Tatverdächtige insgesamt nach Alter und Geschlecht. Bundeskriminalamt, Wiesbaden
- Drescher J (2019) Industrie- und Wirtschaftsspionage in Deutschland. Phänomenologie – materielles Recht – prozessuale Durchsetzung: Bestandsaufnahme und Perspektiven. LIT, Berlin
- Eckert C (2017) Cybersicherheit beyond 2020! Herausforderungen für die IT-Sicherheitsforschung. *Informatikspektrum* 40:141–146
- Franke I, Graf M (2016) Kinderpornografie. Übersicht und aktuelle Entwicklungen. *Forens Psychiatr Psychol Kriminol* 10:87–97
- Honekamp W (2019) Cybercrime: Aktuelle Erscheinungsformen und deren Bekämpfung. In: Lange H-J, Model T, Wendekamm M (Hrsg) Zukunft der Polizei. Forum für Verwaltungs- und Polizeiwissenschaft. VS, Wiesbaden, S 47–59
- Huber E (2019) Cybercrime. Eine Einführung. VS, Wiesbaden
- Huber E, Pospisil B (Hrsg) (2018) Die Cyber-Kriminellen in Wien. Eine Analyse von 2006–2016. Edition Donau-Universität, Krems
- Internet Watch Foundation (IWF) (2018) Pressemitteilung vom 18.04.2018. <https://www.iwf.org.uk/news/iwf-global-figures-show-online-child-sexual-abuse-imagery-up-by-a-third>. Zugriffen: 5. Mai 2020
- Internet Watch Foundation (IWF) (2019) Pressemitteilung vom 24.04.2019. <https://www.iwf.org.uk/news/iwf-launches-once-upon-a-year-and-vows-to-tackle-demand-for-images-of-child-rap>. Zugriffen: 22. Apr. 2019
- Jararweh Y, Al-Ayyoub M, Darabseh A, Benkhelifa E, Vouk M, Rindos A (2015) SDIoT: a software defined based internet of things framework. *J Ambient Intell Human Comput* 6:453–461
- Köllisch T, Jähnke J (2006) Cybercrime gegen Organisationen. Ergebnisse ausländischer Viktimisierungsuntersuchungen und Überlegungen für einen Survey in Deutschland. *Monatsschr Kriminol* 89:366–388
- McAfee (2018) McAfee labs report. December 2018. <https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-dec-2018.pdf>. Zugriffen: 21. Apr. 2020
- Steinmetz KF (2015) Craft(y)ness. An ethnographic study of hacking. *Br J Criminol* 55:125–145
- United Nations Office on Drugs and Crime (UNODC) (Hrsg) (2013) Comprehensive study on cybercrime. Draft, February 2013. https://www.unodc.org/documents/organized-crime/UNODC_CCPJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf. Zugriffen: 21. Apr. 2020
- Ziercke J (2013) Das BKA im 21. Jahrhundert – Neue Herausforderungen, neue Aufgaben. In: Dölling D, Jehle J (Hrsg) Taten – Täter – Opfer. Grundlagenfragen und aktuelle Probleme der Kriminalität und ihrer Kontrolle. Forum Verlag, Godesberg, Mönchengladbach, S 309–325