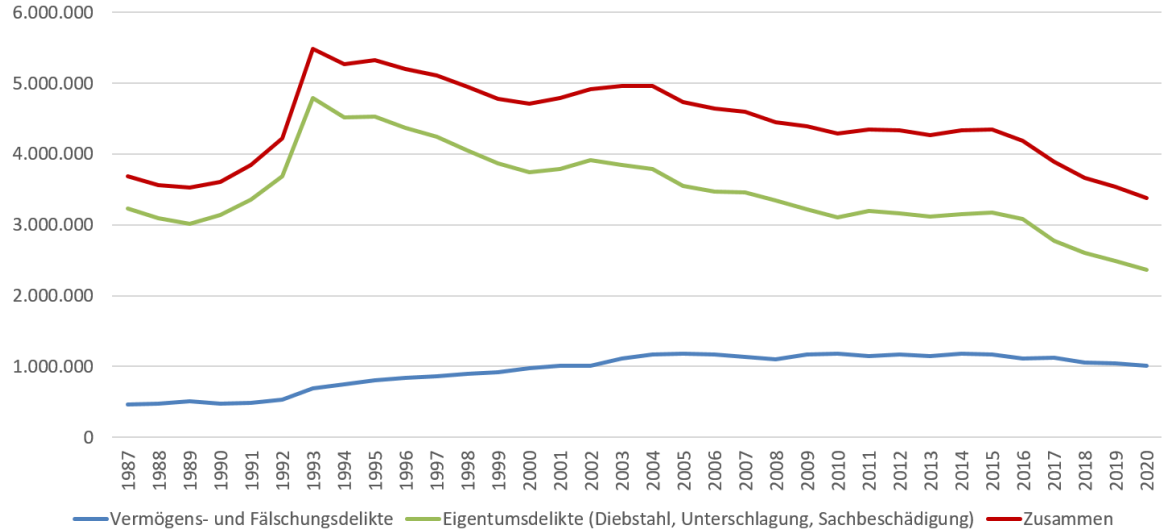
§ 9: Allgemeine Eigentums- und Vermögenskriminalität (Teil 2)

I. Entwicklung der allgemeinen Eigentums- und Vermögenskriminalität

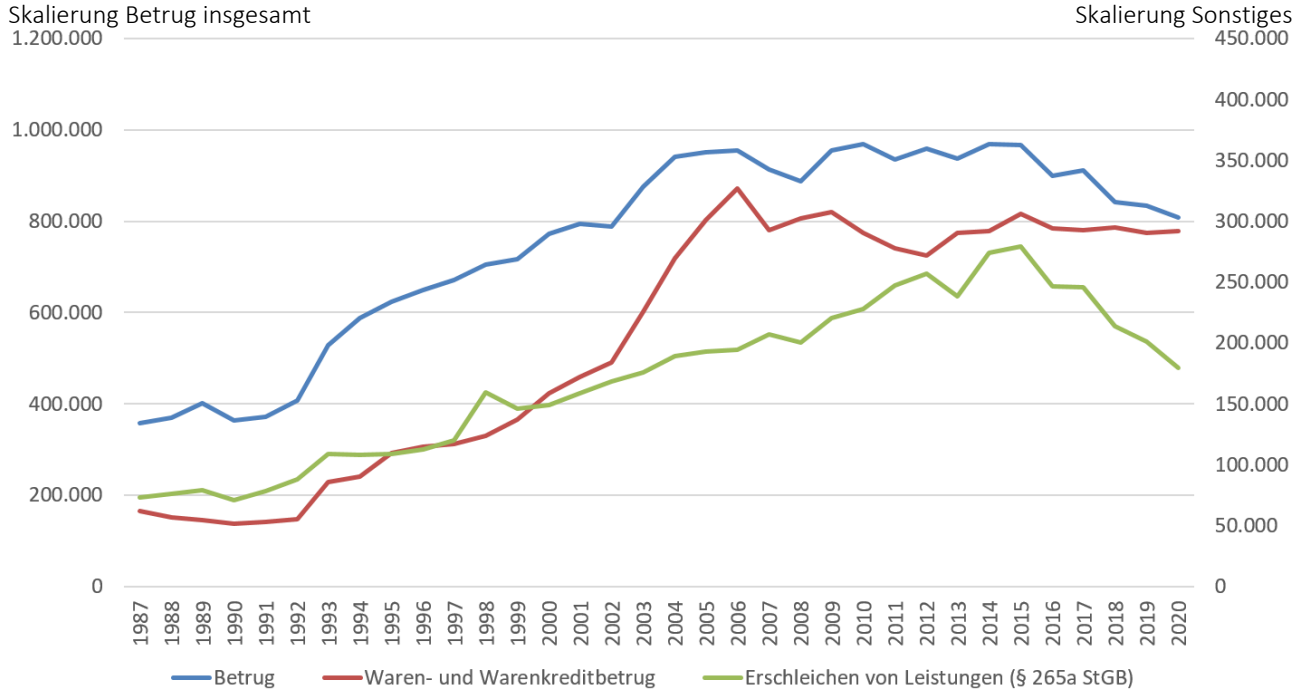
Während Eigentumsdelikte insgesamt mit lediglich geringfügigen Unterbrechungen in den letzten Jahren stark zurückgehen, steigen Vermögensdelikte tendenziell an, wobei in den letzten Jahren eine Stagnation festzustellen ist:

Entwicklung registrierter Eigentums- und Vermögenskriminalität



Quelle: PKS Zeitreihen

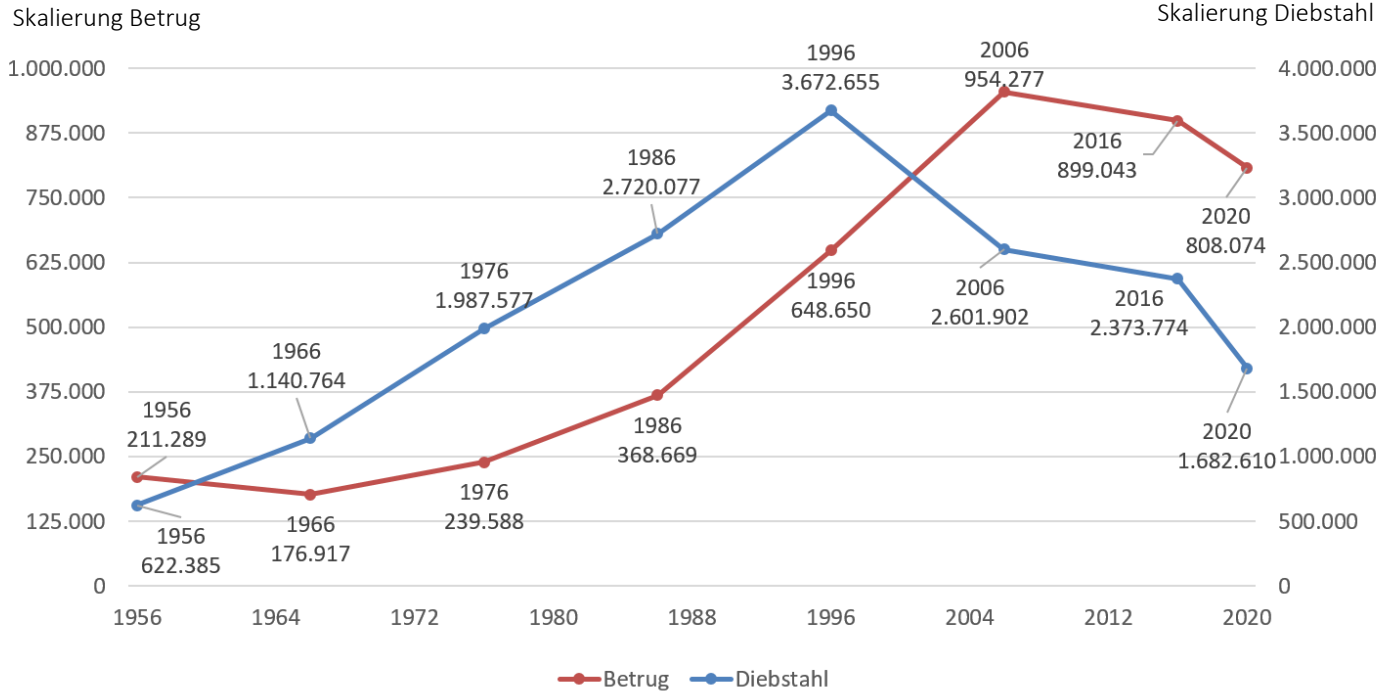
Ein besonders großer Anstieg wurde bei Waren- und Warenkreditbetrug verzeichnet (von 2000 bis 2006 Zunahme um 105,9 % in diesem Bereich; 2006: 327.052 Fälle). Seit 2006 sind die Betrugsfälle in der Tendenz wieder rückläufig (2020: 808.074 Fälle, Abnahme um 15,3 % seit 2006). Auch der Waren- und Warenkreditbetrug ist mittlerweile auf 291.994 Fälle im Jahr 2020 gesunken (Abnahme um 10,7 % seit 2006).



Quelle: PKS Zeitreihen

Bei Betrachtung der gesamten Entwicklung der Nachkriegszeit sind sowohl registrierte Diebstähle als auch Betrug (erst seit den 1970ern) Jahre drastisch angestiegen (Diebstahl bis Mitte der 1990er):

Langzeitentwicklung der Registrierung von Betrug und Diebstahl



Quelle: PKS Zeitreihen

II. Tatmittel Internet als Erklärung?

Eine Erklärung für die über viele Jahre gegenläufige Entwicklung von Eigentums- und Vermögensdelikten liegt möglicherweise im Tatmittel Internet.

Die registrierten Straftaten, die mittels des Internets begangen werden, sind in knapp drei Viertel der Fälle Betrugstaten, mit großem Abstand gefolgt von der Verbreitung pornographischer Schriften (5,4 %) und der Beleidigung (4,5 %). § 242 StGB scheint mit dem vergegenständlichten Tatobjekt „Sache“ im Bereich der virtuellen Welt an Bedeutung zu verlieren. § 303a StGB („Datenveränderung“) ist insofern ein erster Ansatz des Gesetzgebers, der in der Wissenschaft aber auf erhebliche Bedenken stößt (vgl. *Kudlich* Diebstahl und Unterschlagung, in: Hilgendorf/Kudlich/Valerius [Hrsg.], Handbuch des Strafrechts, Band 5, 2020, § 29 Rn. 172: „bedenklich weit gefasst“, „zu unbestimmt“).

Aber auch die klassischen Vermögensstraftatbestände werden nicht lediglich auf neuere Entwicklungen angewendet, sondern stets auch hinsichtlich neuer Tatbegehungsformen mittels des Internets oder Computersystemen angepasst und erweitert. Exemplarisch lässt sich der Computerbetrug gem. § 263a StGB benennen, der 1986 eingeführt wurde, um Betrugsfälle strafrechtlich zu erfassen, bei denen kein Mensch getäuscht wird. Auch das gesetzgeberische Tätigwerden in diesem Bereich mag insoweit zum Anstieg der Fallzahlen beigetragen haben.

1. Erfassung von Straftaten im Internet in der PKS und dem Bundeslagebild Cybercrime

Insbesondere im Bereich der Internetkriminalität ist die kriminalstatistische Aufbereitung des Phänomens auch als ein Versuch der Ermittlungsbehörden zu bewerten, eine breitere Öffentlichkeit auf ausgemachte Gefährdungslagen aufmerksam zu machen (so *Plank* Ist der Begriff „Cyberkriminalität“ in Forschung und Praxis hinreichend konturiert und somit adäquater (Sozial-)Kontrolle zugänglich? in: Rüdiger/Bayerl Cyberkriminologie - Kriminologie für das digitale Zeitalter, 2020, S. 13 [18]).

Die **Polizeiliche Kriminalstatistik** kennt zum einen die Deliktszusammenfassung der **Computerkriminalität** (= Computerkriminalität im engeren Sinne). Hierunter fallen die § 263a, §§ 269, 270 StGB, §§ 303a, 303b StGB, §§ 202a, 202b, 202c StGB sowie die Softwarepiraterie.

Zum anderen werden die **„Straftaten mit dem Tatmittel Internet“** (= Computerkriminalität im weiteren Sinne) in einer Deliktskategorie zusammengeführt. Hierunter werden alle Straftaten erfasst, die auf dem Internet basieren oder mit den Techniken des Internets geschehen. Zur Computerkriminalität im engeren Sinn ergeben sich dabei etwa im Bereich des Computerbetruges Schnittmengen. Erfasst werden aber auch „reguläre“ Straftaten, bei deren Begehung zwar Informationstechnologie genutzt wurde, der Schwerpunkt strafrechtlichen Unrechts jedoch nicht in der Manipulation von Computersystemen liegt. Von Bedeutung sind insoweit insbesondere Betrugsfälle nach § 263 StGB im Bereich des E-Commerce (dazu auch die KK 258), die Verbreitung pornographischer Erzeugnisse sowie Straftaten im Zusammenhang mit Verletzungen des Urheberrechts (§§ 106 ff. UrhG).

Darüber hinaus wird seit 2010 jährlich vom BKA das **Bundeslagebild Cybercrime** veröffentlicht (Ausgabe 2020 hier online abrufbar). Abgebildet werden hier die sog. Cybercrime-Delikte im engeren Sinne (CCieS). Hierzu zählen

- Computerbetrug als Cybercrime im engeren Sinne (§ 263a StGB), hierunter fallen etwa der Betrug mittels rechtswidrig erlangter Daten von Zahlungskarten oder das betrügerische Erlangen von Kfz.
- Missbräuchliche Nutzung von Telekommunikationsdiensten (§ 263a StGB). Das BKA erfasst hierzu Fälle, in denen Sicherheitslücken oder schwache Zugangssicherungen den unberechtigten Zugriff auf Router ermöglicht haben und so gezielt etwa Auslandstelefonieverbindungen angewählt wurden.
- Sonstiger Computerbetrug (§ 263a Abs. 1 und 2 StGB sowie Vorbereitungshandlungen gem. § 263a Abs. 3 StGB)
- Ausspähen und Abfangen von Daten einschl. Vorbereitungshandlungen und Daten-Hehlerei (§§ 202a, 202b, 202c, 202d StGB), erfasst sind damit die Vorstufen zum betrügerischen Einsatz der Daten.
- Fälschung beweiserheblicher Daten bzw. Täuschung im Rechtsverkehr (§§ 269, 270 StGB), worunter etwa die Vortäuschung einer Legende zwecks Erlangung einer Vorkasse-Überweisung auf eBay fällt.
- Datenveränderung/Computersabotage (§§ 303a, 303b StGB): „digitale Sachbeschädigung. Hierunter fällt etwa die Verbreitung von Trojaner, Viren, Würmer usw.).

2. Merkmale der Internetkriminalität

- **Verfügbarkeit von Tatwerkzeugen:** Die zur Begehung von Internetstraftaten notwendigen Tatwerkzeuge sind zumeist frei erhältlich. Der Austausch kinderpornographischer Erzeugnisse bzw. das Herunterladen urheberrechtlich geschützter Werke erfordert nur einen Internetanschluss sowie die geeignete Hard- und Software. Aber auch Softwareprodukte, deren vorrangiger Zweck die Begehung von Straftaten ist (z.B. Programme zur Überwindung von Passwort- oder Kopierschutzmaßnahmen), sind verfügbar. Hier lässt sich in den letzten Jahren eine zunehmende Professionalisierung und Spezialisierung der Anbieterinnen und Anbieter auf online-Marktplätzen im Darknet beobachten (sog. cybercrime as a service).

- **Anonymität:** Vielfältige Möglichkeiten der Anonymisierung (Verwendung öffentlicher Internetterminals, Nutzung von Anonymisierungstechniken [etwa das sogenannte „Tor-Netzwerk"]) erschweren die Rückverfolgung von Straftätern im Internet.

- **Automatisierung:** Der Zahl der über das Internet ausgeführten Angriffe steht vermutlich eine relativ kleine Anzahl von Täterinnen und Täter gegenüber, was auf eine zunehmende Automatisierung von Angriffsprozessen schließen lässt. Dies gilt insbesondere für den Versand von Spam-E-Mails und Hackingangriffen gegenüber öffentlichen Einrichtungen oder Unternehmen. Allein die beiden deutschen Mailanbieter WEB.DE und GMX registrieren im Durchschnitt 150 Millionen Spam-Mails am Tag (vgl. die Statistik auf statista.com hierzu). Allein die Deutsche Telekom registriert bis zu 46 Millionen Cyber-Angriffe pro Tag (vgl. die entsprechende Meldung der Telekom). Solche Zahlen wären durch eine manuelle Ausführung nicht erreichbar und sind

nur durch den Einsatz von Softwaretools zur Automatisierung von Prozessen möglich. Entsprechende Dienstleistungen können ebenfalls auf online-Marktplätzen erworben werden.

- **Transnationalität/Unabhängigkeit von Tat- und Handlungsort:** Der Zugriff auf Inhalte ist infolge der Netzwerkarchitektur weltweit möglich. Die Begehung einer Internetstraftat setzt nicht voraus, dass der Täter oder die Täterin an dem Ort, an dem der Erfolg seiner Tat eintritt, anwesend ist. Zahlreiche Dienstanbieterinnen und Dienstanbieter (cybercime as a service, s.o.), deren Dienste bei der Begehung von Straftaten genutzt werden, bieten ihre Dienste aus dem Ausland an.

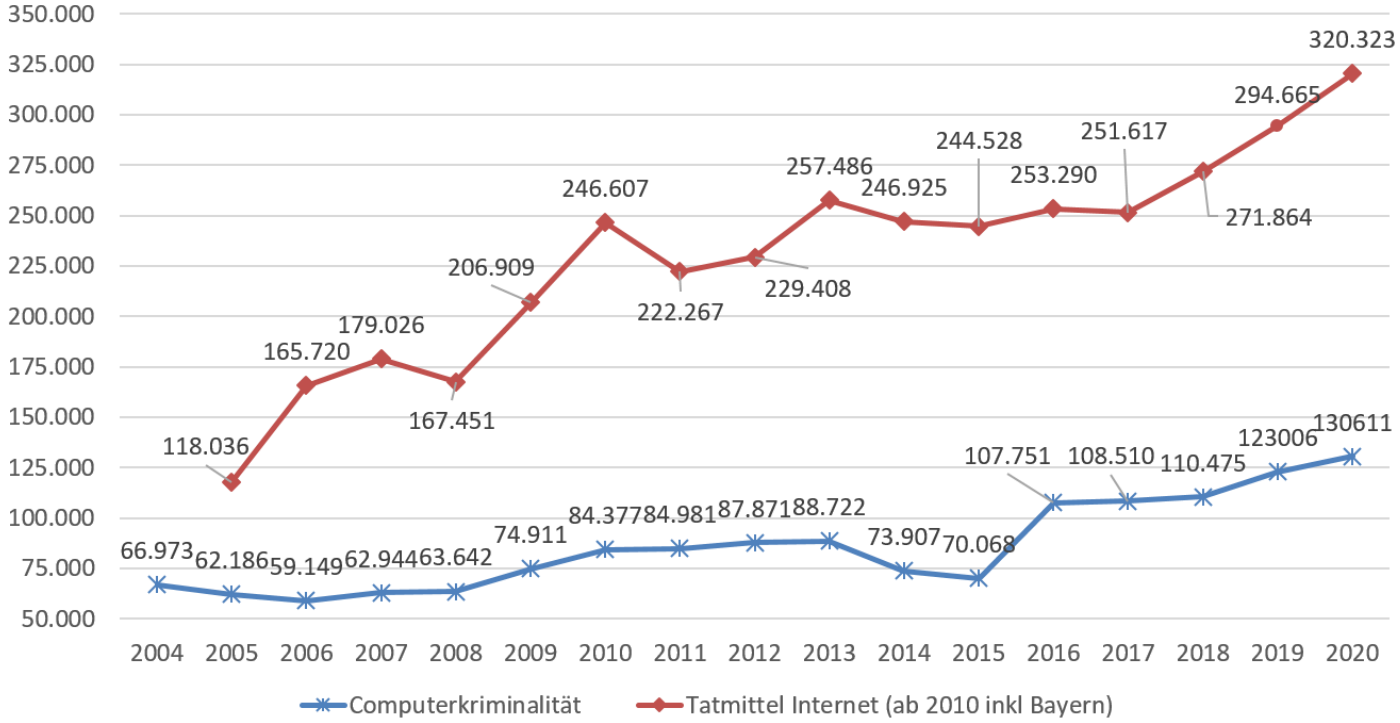
3. Hellfeldbefunde

a) PKS

Die Entwicklung der Straftaten im Bereich der Computerkriminalität verlief in den Jahren 2004–2020 mit Schwankungen, wobei tendenziell ein Anstieg zu verzeichnen ist. In den vergangenen beiden Jahren waren die Anstiege wieder gravierender als in den Jahren zuvor. So wurden für 2020 insgesamt 130.611 Taten erfasst, was einen Anstieg von 6,2 % bedeutet. 2019 war ein Anstieg im Vergleich zum Vorjahr von 11,3 % registriert worden.

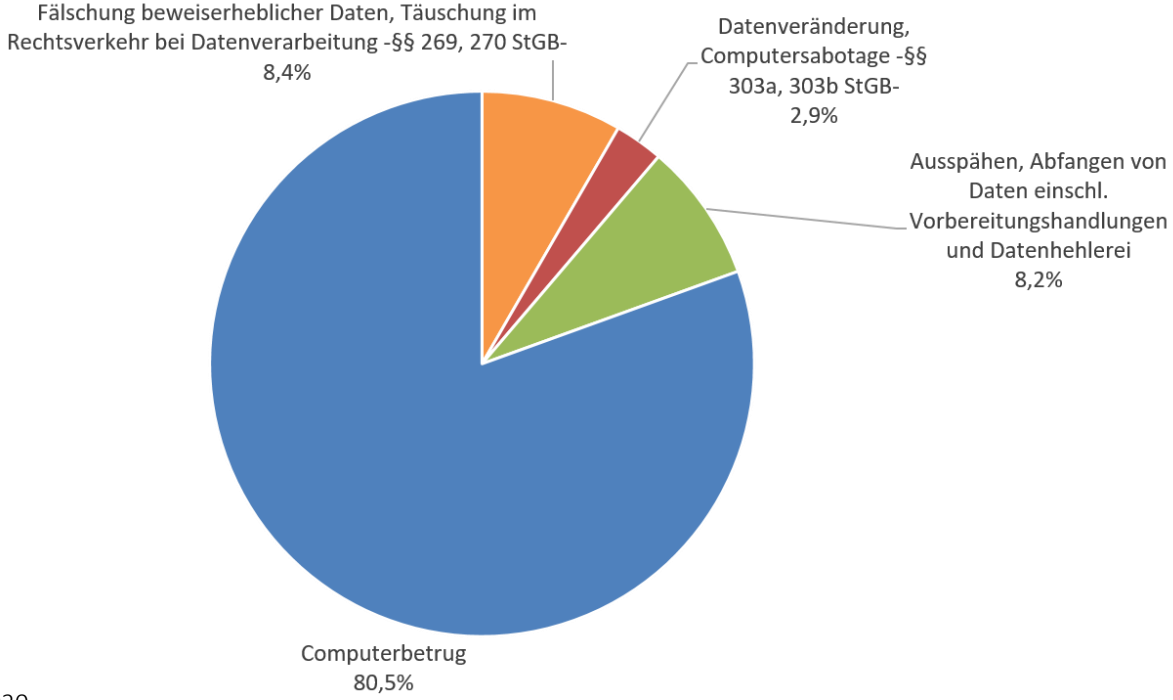
Die Kategorie der Straftaten mit Tatmittel Internet wird in der PKS seit 2005 gesondert dargestellt. Für das Jahr 2020 wurde ein Anstieg der Taten um 8,7 % auf 320.323 Fälle bekanntgegeben. Insgesamt sind bei dieser Deliktskategorie seit ihrer Einführung erhebliche Anstiege zu verzeichnen. Im Vergleich zum Jahr 2005 sind die Straftaten mit dem Tatmittel Internet um 171 % angestiegen. Relativiert wird die Deliktsentwicklung allerdings dadurch, dass in einzelnen Jahren ganze Bundesländer, die zuvor keine gesonderte Erfassung durchführten, in die Statistik erstmalig miteinbezogen worden sind (2010 etwa durch das Land Bayern). So würde sich der 2010 vermerkte Anstieg um 19 % bei einer Nichtbeachtung Bayerns auf ein Plus von 8 % reduzieren.

Entwicklung Fallzahlen Computerkriminalität und Internet als Tatmittel



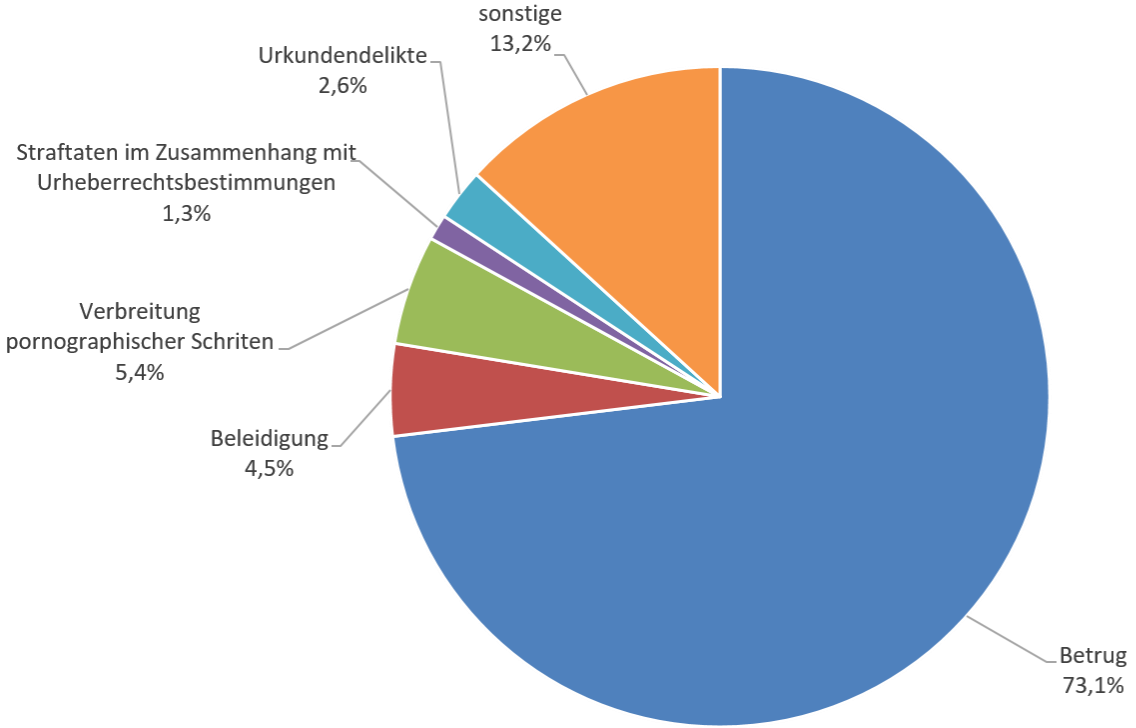
Quelle: PKS 2020

Im Bereich der Computerkriminalität entfallen die größten Anteile registrierter Taten auf den Computerbetrug (80,5 %). Das Ausspähen und Abfangen von Daten einschließlich Vorbereitungshandlungen sowie die Datenhehlerei machen 8,2 % aus. Die Softwarepiraterie spielt im Hellfeld keine große Rolle und beträgt unter 0,5 % der Tatverdachtsfälle im Bereich der Computerkriminalität.



Quelle: PKS 2020

Bei den Straftaten mit Tatmittel Internet dominieren eindeutig Betrugsdelikte (73,1 %).

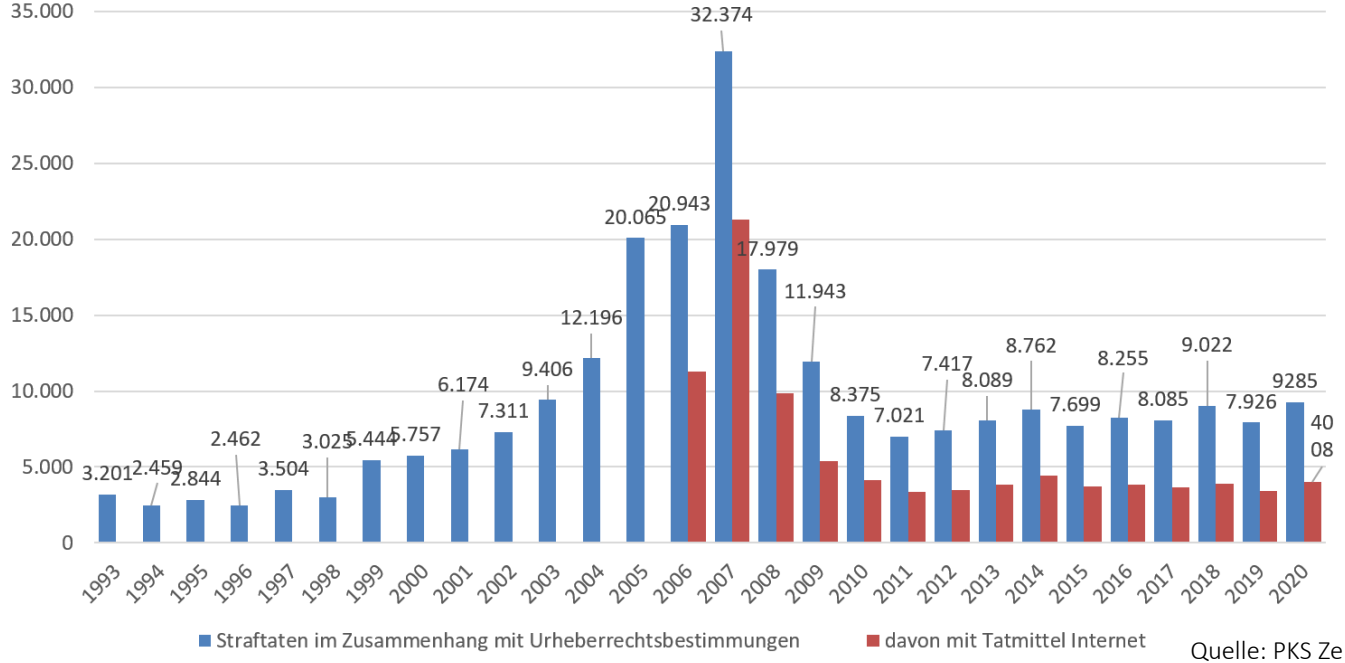


Quelle: PKS 2020

Innerhalb der Betrugsdelikte kommt der größte Anteil dem Waren- und Warenkreditbetrug mit 51,5 % zu.

Obwohl die Straftaten mit dem Tatmittel Internet anstiegen, ist seit einigen Jahren ein erheblicher Rückgang bezüglich der Straftaten gegen das Urheberrecht (inkl. illegale Downloads) zu verzeichnen. Bis 2007 stieg die Fallzahl bei diesen Delikten noch massiv an, was auf technische Entwicklungen zurückzuführen ist: Zum einen gab es in dieser Zeit immer mehr neu geschützte Tatobjekte (z.B. Softwareprodukte), zum anderen sind die Tatbegehungsmöglichkeiten mit der Verbreitung des Internets enorm gestiegen (*Eisenberg/Kölbel* Kriminologie, § 45 Rn. 76).

Seit 2008 sind bei den Straftaten gegen das Urheberrecht wieder enorme Rückgänge zu verzeichnen. Hier liegt die Vermutung nahe, dass es mit der zunehmenden Verbreitung von legalen Streamingdiensten (für Musik [z.B. Spotify], Filme [z.B. Netflix], Hörbücher [z.B. Audible] etc.) sowie illegalen Streaming-Anbietern (bekannt wurde u.a. die Seite „kino.to“) unattraktiver geworden ist, Dateien über Filesharing-Plattformen illegal zu downloaden.

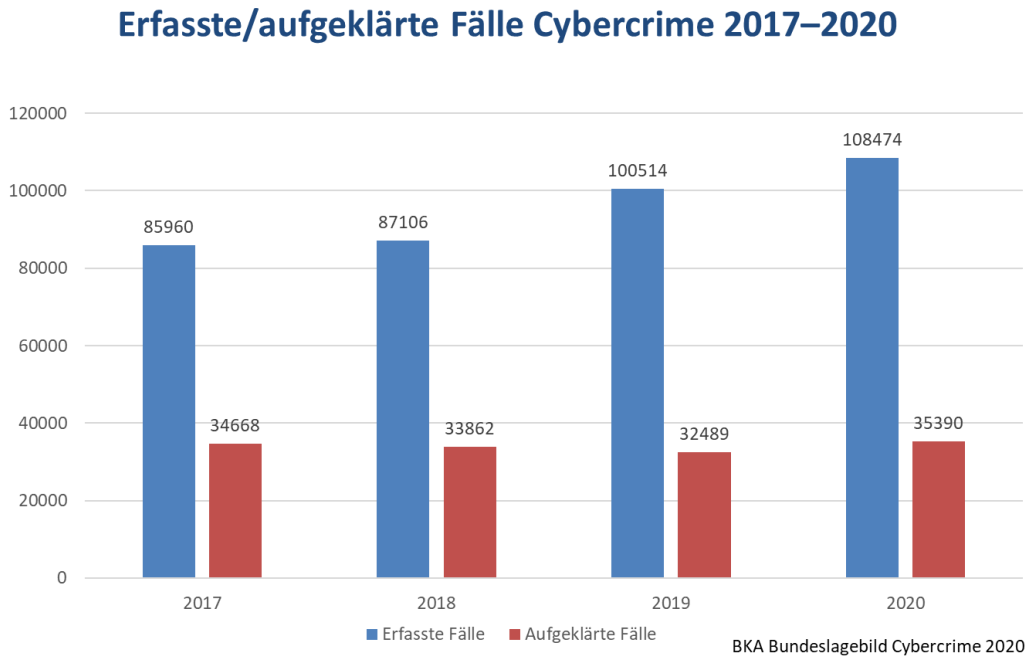


Quelle: PKS Zeitreihen

Dennoch werden nach wie vor 43,2 % der Straftaten gegen das Urheberrecht über das Internet begangen. Die hohen Aufklärungsquoten, 77,9 % bei Urheberrechtsstraftaten insgesamt, 75,7 % bei Tatbegehung über das Internet, sind auf die Musikindustrie zurückzuführen, die speziell nach Verstößen sucht und diese ausnahmslos zur Anzeige bringt.

b) Bundeslagebild Cybercrime

Interessant sind hier unter anderem die Befunde zur Aufklärungsquote bei Cybercrime-Delikten. Während die Zahl der registrierten Fälle Jahr für Jahr ansteigt, stagniert die Anzahl der aufgeklärten Fälle. Dementsprechend sank die Aufklärungsquote von 40,3 % im Jahr 2016 auf 32,6 % im Jahr 2020.



BKA Bundeslagebild Cybercrime 2020

4. Ursachen

Gegenwärtig dominieren auf der Rational-Choice-Theory aufbauende Erklärungsansätze für die Entwicklungen im Bereich der Computerkriminalität (vgl. zu den ökonomischen Kriminalitätstheorien die KK 65 ff. der Kriminologie I-Vorlesung, hier online abrufbar).

Der Anstieg der mit dem Tatmittel Internet verübten Straftaten lässt sich überwiegend mit dem rasanten Bedeutungsgewinn des E-Commerce erklären, infolgedessen große Teile des Geschäftsverkehrs bargeldlos ablaufen. Im Internet abgeschlossene Geschäfte begünstigen dabei die Entstehung betrugsrelevanter Sachverhalte, wobei auf Aspekte der **Routine-Activity-Theory** Bezug genommen werden kann: Tatbereite Personen finden über Online-Kaufportale wie eBay oder Amazon oder Ähnliches eine Vielzahl lohnender Tatobjekte sowie unerfahrene, mit den Gefahren online abgewickelter Kaufverträge nicht vertraute und somit nicht hinreichend geschützte Opfer.

Auch die technische Fortentwicklung von Internet und Computersystemen lässt sich im Sinne **erweiterter Möglichkeiten (Tatgelegenheiten) für Rechtsgutsverletzungen** als Erklärung steigender Fallzahlen heranziehen: So ermöglichen etwa verbesserte Datenübertragungsgeschwindigkeiten den massenhaften Austausch urheberrechtlich geschützter Daten über das Internet.

Der Aussicht, mittels des Ausspähens von Zugangsdaten oder internetbasierenden Betrugsdelikten hohe finanzielle Gewinne einstreichen zu können, steht ein vermeintlich geringer Kostenfaktor entgegen. Zum einen erfordert die Tatbegehung angesichts der generellen Verfügbarkeit von Tatwerkzeugen keinen größeren Aufwand, zum anderen verspricht die Anonymität des Internets Sicherheit vor Identifizierung und strafrechtlicher Verfolgung. Auch die sog. moralischen Kosten (Stichwort: Neutralisierungstechniken, dazu die KK 52 ff. der Kriminologie I-Vorlesung, hier online abrufbar) fallen vergleichsweise gering aus, da das

Tatopfer zumeist gesichtslos bleibt und der verursachte rein finanzielle Schaden eine abstrakte Komponente.

In diesem Zusammenhang wird auch auf die **Broken-Windows-Theorie** Bezug genommen (zu dieser „Theorie" die KK 270 ff. der Kriminologie I-Vorlesung, hier online abrufbar), um die Forderung nach einer stärkeren (polizeilichen) Kontrolle im Netz theoretisch zu unterfüttern. So wie in der realen Welt sichtbare Normverstöße, die nicht zeitnah behoben werden, zu immer weiteren Normverstößen führen sollen, wird derselbe Effekt bei nicht geahndeten Normverstößen im Internet angenommen (*Rüdiger* Das Broken Web: Herausforderungen für die Polizeipräsens im digitalen Raum, in: Rüdiger/Bayerl [Hrsg.], Digitale Polizeiarbeit, 2018, S. 259 [267]). Verschärft werde diese Gefährdungslage im digitalen Raum durch die hier anzutreffende „fixierte Kriminalitätstransparenz": Internetnutzerinnen und -nutzer werden demnach permanent mit scheinbar folgenlosen kriminellen Inhalten und Handlungen konfrontiert, was zu einer Erosion ihrer eigenen Normtreue führen könnte. Während Tatorte in der realen Welt schon kurze Zeit nach der dort begangenen Straftat als solche nicht mehr erkennbar sind, bleiben beispielsweise betrügerische Angebote oder Websites über einen längeren Zeitraum weiterhin online einsehbar (*Rüdiger/Bayerl* Cyberkriminologie – Braucht die Kriminologie ein digitales Upgrade, in: Rüdiger/Bayerl [Hrsg.], Cyberkriminologie – Kriminologie für das digitale Zeitalter, 2020, S. 3 [5 f.]).

5. Gesetzgeberische Reaktion und Strafverfolgung

Die Abhängigkeit heutiger Informationsgesellschaften von der Funktionsfähigkeit ihrer Kommunikationsinfrastruktur (insbesondere IT-Systemen) und die Verletzbarkeit dieser technischen Infrastruktur haben zu einer zunehmenden Einflussnahme des Gesetzgebers auf dieses Gefüge geführt.

Ansätze zur Bekämpfung der Computer- und Internetkriminalität liegen dabei unter anderem in der Verhinderung des Zugangs zu Tatwerkzeugen, etwa zu geeigneter Software. So stellen die Tatbestände der § 263a Abs. 3 StGB bzw. § 202c StGB bereits die Entwicklung einer Software zur Begehung eines Computerbetrugs bzw. die Vorbereitung bestimmter Computerdelikte durch die Erstellung von Programmen unter Strafe. Folge ist eine bedenkliche Überkriminalisierung von Vorbereitungshandlungen im Bereich bestimmter Computer- und Internetdelikte, während die Begehung vergleichbarer Vorbereitungshandlungen außerhalb des digitalen Raumes (noch) keine strafrechtliche Sanktionierung erfährt. Generell lassen sich im Strafrecht aber Vorverlagerungstendenzen in vielen Deliktsfeldern ausfindig machen (vgl. etwa *Puschke* in: Hefendehl [Hrsg.], Grenzenlose Vorverlagerung des Strafrechts, 2010, S. 9–40).

Abseits des materiellen Strafrechts führte das Bemühen zur Bekämpfung der Computer- und Internetkriminalität zu einer Erweiterung strafverfahrensrechtlicher Ermittlungsbefugnisse (§ 100a StPO [Telekommunikationsüberwachung], § 100b StPO [Online-Durchsuchung], § 100g StPO [Verkehrsdatenerhebung], § 100f StPO [Akustische Überwachung außerhalb von Wohnraum] StPO).

Dennoch stellen die speziellen Wesensmerkmale der Computer- und Internetkriminalität sowie deren stetiger technischer Wandel den Strafverfolgungsbehörden nach wie vor besondere Herausforderungen (zur Aufklärungsquote bereits die KK 257). Als Grundproblem stellt sich dabei die dezentrale Netzwerkarchitek-

tur des Internets dar, die äußerst resistent gegenüber jeglichen autoritären Eingriffen und Kontrollversuchen von außen ist. Zur Bewältigung weiterer Probleme der Strafverfolgung werden laufend neu entwickelte, passgenaue Konzepte verfolgt:

- Der Transnationalität vieler Computer- und Internetdelikte und der damit einhergehenden Beschränkung der Strafverfolgungsmöglichkeiten durch das Souveränitätsprinzip soll durch eine enge Verzahnung und Koordinierung der nationalen Behörden sowie einer Harmonisierung nationaler strafrechtlicher Vorschriften begegnet werden.

Auf die Anonymität des Kriminalitätsbereiches wird vermehrt mit der Blockade des Zugangs zu Anonymisierungsservern reagiert. Des Weiteren werden technische Maßnahmen zur Identifizierung des vom Täter tatsächlich genutzten Internetzugangs weiterentwickelt, etwa die Ermittlung der IP-Adresse des Nutzers durch den Einsatz von Cookies. Ebenfalls in diese Richtung geht die Debatte um eine Klarnamenpflicht in sozialen Netzwerken, wie sie beispielsweise die Geschäftsbedingungen von Facebook vorsehen (ein Verfahren hierzu ist beim BGH anhängig). Präventive Maßnahmen zur Vorbeugung von Computer- und Internetkriminalität liegen in der Beobachtung einschlägiger Internetforen durch die Sicherheitsbehörden, der Verbesserung technischer Selbstschutzmaßnahmen durch Behörden und Unternehmen sowie der Schaffung spezialisierter Kooperationseinrichtungen zur Analyse des weltweiten Datenverkehrs (Nationales Cyber-Abwehrzentrum).

Auch jenseits der konkreten Bekämpfung der Internet- und Computerkriminalität nutzen Behörden die Medien zu Zwecken der Aufklärung und Verfolgung von Straftaten in vielfältiger Weise:

- Zugriff auf neue Informationsquellen: Aus der Überprüfung von Computer- und Telekommunikationsdaten versprechen sich Sicherheitsbehörden Hinweise auf begangene oder geplante

Straftaten. Wenngleich die Rechtsgrundlage mancher Eingriffsmaßnahmen (etwa beim Zugriff auf E-Mails) nach wie vor umstritten ist, stellt die Überprüfung von Telekommunikationsdaten eine zentrale Vorgehensweise der Behörden bei der Aufklärung von Straftaten dar. Für das Jahr 2020 wurden im Jahresbericht der Bundesnetzagentur 17,79 Millionen automatisierte Auskunftsersuchen der Sicherheitsbehörden (auf Grundlage des § 112 TKG) verzeichnet. 94 Telekommunikationsunternehmen sind verpflichtet, am Verfahren teilzunehmen. Die Sicherheitsbehörden können also innerhalb kürzester Zeit eine Anfrage bei der Bundesnetzagentur stellen, die Bundesnetzagentur kann automatisch die Daten aus den Kundendateien der Telekommunikationsanbieter abrufen.

- Auf sog. „Internet-Streifen“ überprüfen Ermittlungsbehörden anlassunabhängig Online-Inhalte auf strafrechtlich relevante Hinweise, etwa auch in Gestalt der verdeckten Teilnahme an Kommunikationseinrichtungen (Foren, Soziale Netzwerke etc.). Problematisch erscheinen solche Vorgehensweisen insofern, als die Objekte der staatlichen Ermittlungsbegehrlichkeiten stets besonders grundrechtssensibel sind. So können das heimliche Abrufen, Zusammentragen und Verknüpfen einer Vielzahl von Daten aus unterschiedlichen Lebensbereichen erhebliche Eingriffe in die Grundrechte des Fernmeldegeheimnisses und der informationellen Selbstbestimmung darstellen.

- Neue Ermittlungsmaßnahmen und Zugriffsmöglichkeit: Der Ausweitung staatlicher Zugriffsmöglichkeiten dienen Instrumente wie die Online-Durchsuchung (seit 2017 geregelt in § 100b StPO [strafprozessual] und § 49 BKAG [zur Gefahrenabwehr]), die Quellen-Telekommunikationsüberwachung (geregelt in § 100a Abs. 1 S. 2 StPO [strafprozessual] und § 51 Abs. 2 BKAG

[zur Gefahrenabwehr]) und die Vorratsdatenspeicherung (Neuregelung in § 113b TKG seit 2015). Gegen die genannten Maßnahmen sind jeweils Verfassungsbeschwerden beim BVerfG anhängig (gegen die strafprozessuale Online-Durchsuchung und die Quellen-TKÜ seit August 2018, gegen die Vorratsdatenspeicherung bereits seit 2015). Zudem legte das Bundesverwaltungsgericht im September 2019 die Frage der Vereinbarkeit der deutschen Vorratsdatenspeicherung mit der europäischen „Datenschutzrichtlinie für elektronische Kommunikation" dem EuGH vor. Bis zur endgültigen Klärung ist die Vorratsdatenspeicherung in Deutschland ausgesetzt (vgl. die Pressemitteilung des BVerwG).

- Befugnis für staatlichen Behörden, bestimmte Straftaten zu begehen, um damit Ermittlungsansätze zu erhalten. Seit 2020 ist den Ermittlungsbehörden die Herstellung und Verbreitung fiktiver Kinderpornographie gestattet, um damit Zugang zu entsprechenden Online-Foren zu erhalten (Tatbestandsausschlussfall in § 184b Abs. 6 StGB: Verbreitung, Erwerb und Besitz kinderpornographischer Inhalte). Kritisch hierzu der Beitrag von Thomas Fischer auf Spiegel Online vom 2.1.2020).

- Verfolgungsaufrufe: Zur Herstellung einer umfangreichen Kontrolldichte wird durch den Einsatz von Fernsehen (Aktenzeichen XY) und Internet als Fahndungsmittel eine möglichst breite Öffentlichkeit in die konkrete Strafverfolgung einbezogen.

- Staatliche Reaktion auf private Ermittlungen: Im 2010 ausgestrahlten TV-Format „Tatort Internet (RTL II) wurden reale Straftaten von Privatpersonen provoziert und zum Zwecke der gezielten Diffamierung der Täter ausgestrahlt. Knüpfen staatliche Strafverfahren daran an, besteht neben den ohnehin zu befürchtenden Stigmatisierungswirkungen die Gefahr, dass elementare

Verfahrensgrundsätze – etwa die Beschuldigtenrechte im Ermittlungsverfahren – umgangen werden.

III. Alternative Deutungsrahmen?

Insbesondere die sog. Underground Economy wird in offiziellen Berichten wie dem Bundeslagebild im Cybercrime (dort S. 12 ff.) oder auch in den Medien (vgl. nur die Netflix-Serie „How to sell drugs online (fast)“) wiederholt als eine wesentliche Ausprägung des Kriminalitätsfeldes Cybercrime aufgeführt. Laut BKA handelt es sich bei der Underground Economy um einen „kriminellen Spiegel der realweltlichen und globalisierten Gesellschaft“ (Bundeslagebild Cybercrime, S. 12).

Die hier auf Betrugsdelikte ausgelegten Dienstleistungen („cybercrime as a service“) reichen vom Anbieten digitaler Identitäten, dem Verkauf von gefälschten Inseraten etwa auf eBay oder Amazon, dem Aufsetzen von ganzen Fake-Shops bis hin zu gefälschten Paktversendungsnummern. Insbesondere bei beabsichtigten Betrugstaten gegenüber klassischen Verbraucherinnen und Verbrauchern spielen Kontodaten eine wichtige Rolle. Die Angabe eines Sparkassen- oder Volksbankkontos als Verkäuferkonto lässt ein Online-Angebot wesentlich seriöser erscheinen als etwa die Bezahlmethode PayPal.

Daneben existieren im Darknet auch diverse Angebote an Drogen, Waffen und – entsprechend der momentan omnipräsenten Corona-Pandemie – Impfstoffen (vgl. die Beispiele im Bundeslagebild Cybercrime S. 13 ff.).

In diesem Zusammenhang macht die Studie von *Aldrige* und *Décary-Hétu* auf Aspekte aufmerksam, die in den phänomenologischen Schilderungen des BKA keine Beachtung finden (*Aldrige/Décary-Hétu* Not an „eBay for Drugs“: The Cryptomarket „Silk Road“ as a Paradigm Shifting Criminal Innovation, 2014, hier online abrufbar).

Von der Kriminologin und dem Kriminologen wurden die auf der Darknet-Plattform Silk-Road eingestellten Drogen-Angebote nach Quantität und Preis ausgewertet. Die beiden Forschenden gelangten auf diese Weise zu der Annahme, die Plattform werde insbesondere von Drogendealenden („Handeltreibende“ im Sinne des deutschen BtMG) und nicht von Konsumentinnen und Konsumenten genutzt.

Die Drogenbeschaffung über Online-Marktplätze könnte, so der Ausblick der Studie, zu einer Reduzierung der sonst im Zusammenhang mit Drogengeschäften zu beobachtenden Kollateralschäden in Form von psychischer Gewalt, Erpressungen, Einschüchterungen usw. führen (a.a.O. S. 16).

Die Überlegungen wurden in der Studie von *Barrat/Ferris/Winstock* aufgegriffen (*Barrat/Ferris/Winstock* Safer scoring? Cryptomarkets, social supply and drug market violence, International Journal of Drug Policy 35 (2016), 24 ff., die Zusammenfassung ist hier online abrufbar). Eine Befragung unter Cryptomarket-Nutzerinnnen und -Nutzern (n = 3.794), die auf diese Weise in den letzten 12 Monaten vor der Befragung Drogen bezogen haben, ergaben tatsächlich ein geringeres Vorkommen von Bedrohungen für die eigene Sicherheit (3 % der Befragten) oder Erleben physischer Gewalt (1 % der Befragten) im Vergleich zum Drogenbezug über Freunde/Bekannte (14 % / 6 %), bekannte Dealer (24 % / 10 %) oder Fremde (35 % / 15 %).

Literaturhinweis:

Eisenberg/Kölbel Kriminologie, § 45 Rn. 73–107.

BKA (Hrsg.) Bundeslagebild Cybercrime 2020, 2021.

Zum Darknet etwa *Bachmann*/*Arslan* „Darknet“ Handelsplätze für kriminelle Waren und Dienstleistungen: Ein Fall für den Strafgesetzgeber, NZWiSt 2019, 241.