2 Kriminalitätsbegriff

Die dynamische Entwicklung der Informations- und Kommunikationstechnologie verändert die weltweite Kommunikation, Interaktion und Datenspeicherung tiefgreifend. Damit geht eine entsprechende Veränderung der Erscheinungsformen der IuK-Kriminalität und damit der Tat- und Tätertypologien einher.[36]

Angriffe auf die Integrität und Sicherheit von Datensystemen bergen in unserer modernen Informationsgesellschaft ein hohes Gefahrenpotenzial. Kriminelle können mit einem Mausklick Tausende schädigen.

2.1 Kriminalitätsmerkmale[37]

- Fehlendes Unrechtsbewusstsein und vermeintliche oder tatsächliche Anonymität auf Täterseite fördern die Tatbegehung. Psychologische Hemmschwellen entfallen zunehmend.
- Fehlende Kompetenzen und Technik kaufen oder mieten Täter. Der Kontakt erfolgt über Foren, sodass die Beteiligten in der Regel anonym bleiben. Hierdurch wird das Entstehen internationaler Strukturen begünstigt.
- Täter erschweren den Zugriff der Ermittlungsbehörden, indem sie zunehmend Informationen mit Beweiswert nicht auf ihrem Rechner, sondern im Internet speichern. Sie nutzen Internettelefonie (VolP) über internationale Anbieter, Kryptierungstechniken sowie Steganografie und verschleiern IP-Adressen.
- Täter reagieren sehr schnell auf technische Sicherheitsvorkehrungen, indem sie unverzüglich ihre Vorgehensweise durch Anpassung der Schadprogramme ändern. Dadurch entfalten Sicherheitsvorkehrungen in der Regel nur kurzzeitig Wirkung.
- Das Dunkelfeld im Bereich der IuK-Kriminalität im engeren Sinne ist hoch einzuschätzen. In vielen Fällen wird die Straftat vom Geschädigten nicht bemerkt. Bei Wirtschaftsbetrieben ist ein befürchteter Imageverlust häufig Ursache für eine Nichtanzeige.

36 Programm Innere Sicherheit, vgl. FN 35. Hier wird der bis dahin gebräuchliche Begriff „IuK-Kriminalität“ verwendet.

37 Programm Innere Sicherheit, vgl. FN 35.

2.2 Begriff Cybercrime

Im politischen, wirtschaftlichen, gesellschaftlichen und polizeilichen Sprachgebrauch begann sich der Begriff Cybercrime zu formen. Gemäß der am 01.07.2009 in Kraft getretenen „Convention on Cybercrime" des Europarates[38] – Deutschland ratifizierte die EU-Konvention am 09.03.2009 – sind die nachfolgenden Straftaten vom Begriff Cybercrime umfasst[39]:

1. **Straftaten gegen die Vertraulichkeit, Unversehrtheit und Verfügbarkeit von Computerdaten und -systemen** – 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** – 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** – Straftaten, bei denen über das Netz illegale Inhalte transportiert werden, also Informationen, deren Umgang vom Gesetzgeber mit Strafe bedroht wird, z. B. Kinderpornografie, Gewaltdarstellungen und Propagandadelikte.
4. **Straftaten im Zusammenhang mit Verletzungen des Urheberrechts und verwandter Schutzrechte** – 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** – gem. Zusatzprotokoll 2006.

38 Convention on Cybercrime, Budapest, 23.11.2001 (CETS No. 185), übersetzt als „Übereinkommen über Computerkriminalität".

39 Weiter dazu *Meier*, Neue Kriminalitätsformen: Phänomenologie und Bedingungsfaktoren der Internetkriminalität, in: Hilgendorf/Regnier (Hrsg.), Festschrift für Wolfgang Heinz zum 70. Geburtstag, 2012.

Der Arbeitskreis II „Innere Sicherheit“ (AK II)[40] sah vor dem Hintergrund nationaler sowie internationaler sicherheitspolitischer Entwicklungen das Erfordernis, den phänomenbezogenen Sprachgebrauch zu harmonisieren und die bisherigen Begriffsbestimmungen zur „IuK-Kriminalität“ durch den Begriff „Cybercrime“ zu ersetzen. Es gilt die nachfolgende Definition.

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.

Diese Begriffsbestimmung berücksichtigt sowohl nationale[41] als auch internationale Sicherheitsstrategien und steht im Einklang mit internationalen Begriffsbestimmungen wie der Convention on Cybercrime[42], der United Nations Organization[43] und des FBI[44].

Sie ist geeignet, alle Straftaten der Cybercrime, sowohl der bisher als IuK-Kriminalität im engeren Sinn bezeichneten Delikte als auch der Straftaten, bei denen die IuK als Tatmittel verwendet wird (bislang als IuK-Kriminalität im weiteren Sinn bezeichnet), abzubilden. Der besonderen Bedeutung des Internet als wichtigstes Datennetz im Zusammenhang mit der Cybercrime wurde durch eine explizite Nennung in der Definition Rechnung getragen.

Auf eine Unterscheidung zwischen Cybercrime im engeren Sinne und sonstiger Cybercrime wurde verzichtet, da die Definition das Phänomen Cybercrime als Ganzes beschreiben soll. Gleichwohl erlaubt die Definition eine solche Differenzierung, was u. a. die praktische Umsetzung erleichtern wird (fachlich richtige und bekannte phänomenologische Zuordnung[45]).

Eine einheitliche Definition des Begriffs Cybercrime war auch erforderlich, weil er sowohl im öffentlichen als auch im privaten Raum zunehmend Ver-

40 Arbeitskreises II „Innere Sicherheit“ der Ständigen Konferenz der Innenminister und -senatoren der Länder/IMK.

41 Cyber-Sicherheitsstrategie für Deutschland, Bundesministerium des Innern/BMI, 2011 – beinhaltet u. a. Ausführungen zur Gefährdungslage und zu strategischen Zielen und Maßnahmen.

42 Convention on Cybercrime des Europarates, vgl. oben.

43 Vereinte Nationen/UNO (United Nations Organization), Organisation der Vereinten Nationen.

44 Federal Bureau of Investigation, Ermittlungsbehörde des US-Justizministeriums.

45 Vgl. Kapitel 2.3 und 2.4.

wendung findet, im internationalen Kontext gebräuchlich ist und auch von der Polizei (z. B. bei Medienkontakten, in der Öffentlichkeitsarbeit) genutzt wird.

Der Begriff Cybercrime löst damit die bisher verwandte Bezeichnung „Informations- und Kommunikationskriminalität (IuK-Kriminalität)“ ab.

2.3 Cybercrime im engeren Sinn

Es handelt sich um Straftaten, bei denen **Informations- und Kommunikationstechnik – Elemente der EDV – in den Tatbestandsmerkmalen der Strafnorm** enthalten ist (Computerkriminalität).

Zunächst beinhaltete Cybercrime im engeren Sinn im Wesentlichen Kriminalitätsformen wie die Manipulation von Telefonkarten, die missbräuchliche Verwendung von Telefonanlagen sowie den betrügerischen Einsatz von „Dialern“ und Mehrwertdiensten. Zwischenzeitlich wird dieser Phänomenbereich zu mehr als 90 % durch das widerrechtliche Abgreifen von Daten, das sogenannte „Phishing“, dominiert. Ursprünglich zielten „Phishing-Angriffe“ nur auf wenige Geschäftsbereiche der Netz-Welt, vornehmlich Banken und Auktionsplattformen. Das Zielspektrum der Täter hat sich mittlerweile wesentlich erweitert. Es werden nicht mehr nur die Zugangsdaten eines Opfers ausgespäht, sondern seine gesamte „Digitale Identität“ (DI).

Die erlangten Daten werden auf einem globalen Marktplatz, der sogenannten „underground economy“, vermarktet. Gehandelt werden hier auch kriminelle Geschäftsmodelle, Schadprogramme und Infrastrukturen. Der illegale Markt orientiert sich wie „normale“ Märkte an den Kundenbedürfnissen und damit vor allem an der Nachfrage.

Ein besonders starker Anstieg der registrierten Cybercrime im engeren Sinn ist in den Bereichen „Ausspähen von Daten, Datenveränderung/-fälschung und Rechnersabotage“ zu verzeichnen.

Weitere Erscheinungsformen der Cybercrime im engeren Sinne sind:

– Einsatz von Schadprogrammen, z. B. „Malware“ und Trojaner, als Tatmittel zum Angriff auf Rechner und auf Mobiltelefone
– Nutzung sogenannter „Botnetze“ zur Verschleierung oder Anonymisierung von Täteraktivitäten[46]

46 Vgl. Kapitel 17, Botnetz.

– Überlastung von Servern mit massenhaften Anfragen, um zu verhindern, dass dessen Inhalte verfügbar sind („DDoS-Angriffe“)
– unberechtigtes Eindringen in Rechnersysteme („Hacking“).[47]

Tatbestände der Cybercrime im engeren Sinn sind nachfolgend aufgeführt.

2.3.1 Straftaten nach dem Strafgesetzbuch (StGB)

Die Bestimmungen wurden durch das **41. Strafrechtsänderungsgesetz** zur Bekämpfung der Computerkriminalität – in Kraft getreten am 11.08.2007 – aktualisiert. Die Änderungen beruhten auf dem EU-Rahmenbeschluss über Angriffe auf Informationssysteme und dem Übereinkommen des Europarats über Computerkriminalität. Zu berücksichtigen sind insbesondere (vgl. Kapitel 20.1):

– § 149 StGB – Vorbereitung der Fälschung von Geld und Wertzeichen
– § 202a StGB – Ausspähen von Daten (sog. „elektronischer Hausfriedensbruch“)
– § 202b StGB – Abfangen von Daten
– § 202c StGB – Vorbereiten des Ausspähens und Abfangens von Daten
– § 263a StGB – Computerbetrug
– § 269 StGB – Fälschung beweiserheblicher Daten
– § 270 StGB – Täuschung im Rechtsverkehr bei Datenverarbeitung
– § 271 StGB – Mittelbare Falschbeurkundung
– § 274 StGB – Urkundenunterdrückung
– § 303a StGB – Datenveränderung
– § 303b StGB – Computersabotage

Die Delikte sind auch Bestandteil des **Sondermeldedienstes Cybercrime** (SMD Cybercrime) in den Ländern und dem Bund.[48]

Qualifizierte Tatbestände für schwerwiegende und breitflächige Angriffe auf Informationssysteme und beim Ausspähen von Daten können in den Tatbeständen §§ 202a, 202b und 303a StGB berücksichtigt werden. Die §§ 202a, 202b und 303a StGB sollten auch eine Möglichkeit der Sanktionierung eines Versuchs (§ 22 StGB) vorsehen.[49]

47 Vgl. FN 35.

48 Vgl. Cyberkriminalität/Digitale Spuren, Jahresbericht, LKA Baden-Württemberg, 2013.

49 *Bär*, Rechtliche Herausforderungen bei der Bekämpfung von Cybercrime, BKA-Herbsttagung „Cybercrime – Bedrohung, Intervention, Abwehr“, 2013; vgl. www.bka.de.

Mit Einführung des § 202d StGB ist auch das „Sichverschaffen“ nicht allgemein zugänglicher Daten, die ein anderer rechtswidrig erlangt hat, als „Datenhehlerei“ strafbar.[50]

2.3.2 Urheberrechtsverletzungen, Softwarepiraterie – Gesetz über Urheberrecht und verwandte Schutzrechte (UrhG)

Das Kopieren von geschützten Werken ist generell verboten. Nach § 95a UrhG dürfen wirksame technische Maßnahmen ohne Zustimmung des Rechtsinhabers nicht umgangen werden. Schutzgut der Straftatbestände des Urheberrechts sind insbesondere die Verwertungsrechte des Berechtigten. Zu beachten sind (vgl. Kapitel 20.2):

- § 95a UrhG – Schutz technischer Maßnahmen
- § 106 UrhG – Unerlaubte Verwertung urheberrechtlich geschützter Werke
- § 107 UrhG – Unzulässiges Anbringen der Urheberbezeichnung
- § 108 UrhG – Unerlaubte Eingriffe in verwandte Schutzrechte
- § 108a UrhG – Gewerbsmäßige unerlaubte Verwertung
- § 108b UrhG – Unerlaubte Eingriffe in technische Schutzmaßnahmen und zur Rechtewahrnehmung erforderliche Informationen
- § 109 UrhG – Strafantrag
- § 110 UrhG – Einziehung
- § 111a UrhG – Bußgeldvorschriften

2.3.3 Verstöße gegen das Telekommunikationsgesetz (TKG)

Zweck des Gesetzes ist es, durch technologieneutrale Regulierung den Wettbewerb im Bereich der Telekommunikation und leistungsfähige Telekommunikationsinfrastrukturen zu fördern und flächendeckend angemessene und ausreichende Dienstleistungen zu gewährleisten.

Ziele sind unter anderem die Wahrung der Nutzer-, insbesondere der Verbraucherinteressen auf dem Gebiet der Telekommunikation, die Wahrung des Fernmeldegeheimnisses und die Wahrung der Interessen der öffentlichen Sicherheit. Grundsätzliche Regelungen zum Datenschutz beinhaltet in Teil 7 des Gesetzes der Abschnitt 2. Im Abschnitt 3 des gleichen Teils

50 Eingefügt mit dem Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten vom 10.12.2015 (BGBl. I S. 2218), in Kraft getreten am 18.12.2015.

finden sich Vorgaben für die Anbieter von Telekommunikationsdiensten und Regelungen für Auskunftsersuchen von Sicherheitsbehörden.

Die **§§ 148, 149 TKG** beinhalten die **Straf- und Bußgeldvorschriften**.

2.4 Cybercrime im weiteren Sinn

Dies sind Straftaten, bei denen **Informations- und Kommunikationsmedien zur**

- **Planung und/oder**
- **Vorbereitung und/oder**
- **Ausführung**

eingesetzt werden.

Es handelt sich um Straftaten, die mit dem **Tatmittel Internet** begangen werden.

Nahezu jede strafbare Handlung kann durch den Einsatz solcher Technik „effektiviert" werden. Die Deliktsbreite reicht von der Verbreitung kinderpornografischer Inhalte über das betrügerische Anbieten von Waren und Dienstleistungen, das verbotene Glücksspiel, unlautere Werbung, Urheberrechtsverletzungen bis zum illegalen Verkauf von Waffen, Betäubungsmitteln und Medikamenten und zu Beleidigungen/Bedrohungen im Chat oder per E-Mail. Darüber hinaus nutzen terroristische Netzwerke, extremistische Gruppierungen sowie Organisierte Kriminalität und Wirtschaftskriminalität die IuK-Technik als Plattform für

- Information und Kommunikation
- Propaganda durch Hetz- und Schmähschriften mit dem Ziel der Radikalisierung und/oder der Bedrohung von „Gegnern"
- Verbreitung von Handlungsanleitungen, auch zum Bau und Einsatz von Sprengvorrichtungen/-fallen
- Rekrutierungen und Anmietungen
- Tatmittelbeschaffung.

2.5 Täterstruktur

Die **Tätertypen** sind höchst unterschiedlich, ihre Motivlagen und ihr technisches Können sind äußerst different. Vom Einsteiger bis zum Profi sind

alle vertreten: Jugendliche Hacker, die ihr Potenzial testen wollen, Extremisten, Erpresser, Terroristen, lose kriminelle Strukturen und Banden, international organisierte Kriminelle, Nachrichtendienste anderer Staaten.

Als Einsteiger sehen wir[51] **Cyberkriminelle mit IT-Grundkenntnissen** oder auch sogenannte Script Kiddies. Mit vorprogrammierten Software-Toolkits beschäftigen sie sich überwiegend mit Phishing, im Bereich Social Engineering und im Defacement, also dem Verändern von Webseiten. Dieser Gruppe geht es vor allem darum, Erfahrungen zu sammeln und die breiten Möglichkeiten des Internet zu erproben.

Deutlich gefährlicher sind **fortgeschrittene Hacker** mit einer **hohen Affinität zur Technik**. Von ihnen gehen strukturierte Attacken, wie DDoS, Drive-by-exploit oder SQL-Injections aus. Die Akteure sind Hobby-Hacker, ideologische Hacker oder organisierte Gruppen. Diese Gruppe verfügt über gute IT-Kenntnisse, die es ihr ermöglichen, an persönliche Daten, betriebsinterne Informationen oder vertrauliche Regierungsdokumente zu gelangen.

Die dritte Gruppe sind die „**Profis**“. Hier finden sich sowohl **staatlich gelenkte Hacker** als auch **terroristische Gruppen** und **Hacktivisten**. Hacktivisten verstehen sich als Kämpfer gegen Ungerechtigkeit, verstehen ihr Handeln als zivilen Ungehorsam gegen bestimmte politische Richtungen – ein virtueller Gang auf die Straße, um Unternehmen, Regierungsbehörden, Parteien, andere Gruppen oder Initiativen von ihrem – in den Augen von Gruppen wie Anonymous oder Lulz-Security falschen – Weg abzubringen. Mittels DDos-Attacken werden Internet-Portale lahmgelegt oder es werden Datenbanken gehackt, um im Anschluss „sensible“ Informationen zu veröffentlichen. Es handelt sich um eine andere Qualität von Internetangriffen. Es geht darum, einen möglichst großen Schaden anzurichten, der Profit ist eher ideeller Natur.

Der überwiegende Teil der Cyberkriminellen handelt aus finanzieller Motivation. Dabei reicht das Spektrum vom klassischen Einzeltäter bis hin zu international organisierten Tätergruppierungen. Täter arbeiten im Bereich Cybercrime oftmals nicht mehr in den klassischen hierarchischen Strukturen, sie kennen sich teilweise nicht persönlich, sondern nutzen auch bei arbeitsteiliger Kooperation die Anonymität des Internets.

Services, die nicht selbst erbracht werden können, werden von anderen hinzugekauft. Das Angebot in der Underground Economy ist breit und

51 *Ziercke*, Kriminalistik 2.0 – effektive Strafverfolgung im Zeitalter des Internet aus Sicht des BKA, BKA-Herbsttagung, 2013, www.bka.de, 22.05.2020.

reicht von für die Begehung von Straftaten erforderlicher Schadsoftware bis hin zu kompletten technischen Infrastrukturen.[52]

2.6 Kriminologische Einordnung

In der Kriminologie[53] wird der Begriff „Cybercrime“ kritisch gesehen.

Übernommen aus dem anglo-amerikanischen Sprachgebrauch wird er wohl deshalb gerne verwendet, weil er auf den „Cyberspace“ verweist, jenen in der 1990er Jahren von vielen Internetnutzern imaginierten virtuellen Raum, in dem man sich ähnlich wie in einem dreidimensionalen Raum aufhalten und im Austausch mit anderen Nutzern neue Erfahrungen sammeln kann. Die Aussage „immer mehr Straftaten finden nicht mehr auf der Straße, sondern im Internet statt“ erweckt dabei den Eindruck, das „Internet“ sei ein Raum eigener Art, der als Tatort in der gleichen Weise in Betracht kommt wie „die Straße“. Dass das Internet keinen eigenen Erlebnisraum eröffnet, sondern lediglich das Medium für neue, erweiterte Informations- und Kommunikationsformen darstellt, dürfte indes heute – ungeachtet eines nach wie vor abweichenden Sprachgebrauchs – weitgehend Allgemeingut sein. Für die kriminologische Analyse sollte der die Zusammenhänge verklärende Kunstbegriff des „Cybercrime“ deshalb eher vermieden werden.[54]

Die Erklärung der Internetkriminalität scheint ohne Anleihen bei den herkömmlichen Kriminalitätstheorien nicht auszukommen. Vertiefende Analysen der Zusammenhänge mit Risiko- und Schutzfaktoren oder den Auswirkungen der im Internet begangenen Straftaten sind noch Mangelware.[55]

Der Gesichtspunkt der Kontrolle spielt sicherlich eine herausgehobene Rolle, so die fehlenden Selbstschutzmaßnahmen der Geschädigten (z. B. Phishing), die nicht ausreichenden Überwachungsmaßnahmen der Strafverfolgungsbehörden bei den abstrakten Gefährdungsdelikten (z. B. Kinderpornografie) oder die eingeschränkte Selbstkontrolle der Täter. Auch Kosten-Nutzen-Erwägungen auf der Täter- wie der Opferseite, z. B. der Aufwand bei der legalen Beschaffung von immateriellen Gütern wie Filmen und Musik oder der Aufwand bei der Installation von Sicherheitssoftware,

52 Vgl. BKA, Cybercrime Bundeslagebild 2015, www.bka.de, 22.05.2020.

53 Kriminologie als Lehre von den Ursachen und Erscheinungsformen von Kriminalität, vgl. Handbuch für die Ausbildung der Polizei Baden-Württemberg, Fachteil K, Richard Boorberg Verlag.

54 *Meier*, vgl. FN 39.

55 *Meier*, vgl. FN 39.

ebenso Lerneffekte, Neutralisierungsmechanismen und Routineaktivitäten, sind von Bedeutung.[56]

In einem Erklärungsmodell müssen auch die Besonderheiten integriert werden, die sich aus der Nutzung der IuK-Technik als Tatmittel ergeben. Warum ist gerade das Internet für die Begehung von Straftaten ein so geeignet erscheinendes Medium?

Welche Umstände erleichtern die Tatbegehung gegenüber Taten in der „realen" Welt? Im Zusammenhang mit Cybersex[57] wird das Internet als „Triple-A-Engine" bezeichnet – gekennzeichnet durch Verfügbarkeit (accessability), Erschwinglichkeit (affordability) und Anonymität (anonymity). Die durch das Netz geschaffene Distanz zwischen Täter und Opfer mit ihren Folgen sowohl beim Täter als auch beim Opfer (Herabsetzung von Hemmschwellen, Verdrängung der Gefahr) bedürfen der Thematisierung. Täter- und Opferrollen werden durch Zwischenschaltung des Mediums Internet undeutlicher – wer ist bei dem Umgang mit Kinderpornografie der Täter – derjenige, der das Material über das Internet verbreitet, der es herunterlädt, oder beide? Wer ist bei DDos-Angriffen das Opfer? Derjenige, auf dessen PC ein Botnetz installiert wird, derjenige, dessen Server lahmgelegt wird, oder beide?

Welche Auswirkungen hat die im Internet erfahrene Viktimisierung auf die Opfer? Ist „Cyberbullying" oder die nicht rückgängig zu machende Verbreitung identifizierenden pornografischen Bildmaterials wegen der weltweit unbegrenzten Wahrnehmbarkeit durch Dritte für die Betroffenen ein stärkerer Eingriff, als es vergleichbare Taten in der „realen" Welt sind? Welche Konsequenzen ergeben sich aus der Untrennbarkeit der erfahrenen Demütigung für die Opferbehandlung und die Prävention?

Die Fragen zeigen, dass die kriminologische Auseinandersetzung noch ganz am Anfang steht.[58]

„Gamecrime und Metacrime"[59] bezeichnen Kriminalität im Zusammenhang mit virtuellen Spielwelten. Es handelt sich um Straftaten im Zusammenhang mit Online-Rollenspielen (Games), wie z. B. „World of Warcraft",

56 *Meier*, vgl. FN 39.

57 Vgl. auch *Beutel*, Sexualität online: riskantes Verhalten, Cybermobbing, Onlinesexsucht, Die Kriminalpolizei, 3/2013.

58 *Meier*, vgl. FN 39.

59 *Krebs/Rüdiger*, Gamecrime und Metacrime – Strafrechtlich relevante Handlungen im Zusammenhang mit virtuellen Welten, 2010. Die Verfasser behandeln in ihrer an der Universität Hamburg im Studienfach Kriminologie vorgelegten Abschlussarbeit kriminelle Erscheinungsformen, das Aufkommen im Hell- und Dunkelfeld und deren Vergleichbarkeit zu denen der realen Welt, rechtliche Erörterungen und kriminologische Erklärungsansätze.