



Cyberkriminalität im Kontext von Partnerschaft, Sexualität und Peerbeziehungen: Zur Cyberkriminologie des digitalen sozialen Nahraums

Martin Rettenberger^{1,2} · Fredericke Leuschner¹

Eingegangen: 24. Mai 2020 / Angenommen: 2. Juni 2020 / Online publiziert: 25. Juni 2020
© Der/die Autor(en) 2020

Zusammenfassung

Die Etablierung des Internets als sozialer Raum stellte die größte Umwälzung menschlicher Kommunikations- und Interaktionsformen der letzten Jahrzehnte dar, wodurch altbekannte Delinquenzformen an die digitale Welt angepasst wurden, aber auch neue kriminalitätsbezogene Äußerungsformen entstanden. Der vorliegende Übersichtsartikel beschäftigt sich vorrangig mit kriminologischen und forensischen Erkenntnissen aus dem deutschsprachigen Raum zu Formen der Cyberkriminalität, die im Kontext von Partnerschaft, Sexualität und Peerbeziehungen auftreten: Neben dem Cyberstalking und Cybergrooming werden Cyberbullying (oder -mobbing) sowie das (Love- oder Romance-)Scamming kurz vorgestellt und zentrale Forschungsergebnisse referiert. Die Darstellung dieser cyberkriminellen Ausdrucksformen verdeutlicht den stetigen Zuwachs an Bedeutung, den dieser Delinquenzbereich in den letzten Jahren verzeichnete, und unterstreicht gleichzeitig die Notwendigkeit einer spezifischen Cyberkriminologie dieser und anderer digitalen Delinquenzformen.

Schlüsselwörter Internetkriminalität · Cyberstalking · Cybergrooming · Cyberbullying · Scamming

Cybercrime in the context of partnerships, sexuality and peer relationships: The cybercriminology of digital social proximity

Abstract

The establishment of the internet as a crucial social area is undoubtedly one of the most relevant transformations of human communication and interaction expressions in the last decades, whereby well-known forms of crime have been adapted to the digital age. At the same time, new manifestations of delinquent behavior have arisen. This review article deals primarily with criminological and forensic research results from the German-speaking area about cybercrime types, which occur in the areas of partnerships, sexuality and peer relationships. The phenomena of cyberstalking, cybergrooming, cyberbullying (or cybermobbing) and (love or romance) scamming are introduced and central research results from the German-speaking countries are reported. The presentation of these current manifestations of cybercrime underlines the steady increase of the relevance and importance of this area of delinquency in the last few years and at the same time highlights the necessity of a specific cybercriminology of these and other forms of digital delinquency.

Keywords Internet crime · Cyberstalking · Cybergrooming · Cyberbullying · Scamming

✉ Prof. Dr. Martin Rettenberger
m.rettenger@krimz.de

¹ Kriminologische Zentralstelle (KrimZ),
Viktoriastraße 35, 65189 Wiesbaden, Deutschland

² Psychologisches Institut, Johannes Gutenberg-Universität
(JGU), Mainz, Deutschland

Einleitung

Die Etablierung des Internets als sozialer Raum stellte die größte Umwälzung menschlicher Kommunikations- und Interaktionsformen der letzten Jahrzehnte dar (Rüdiger und Bayerl 2020). Mehr als die Hälfte der Menschheit nutzt regelmäßig das Internet, ein großer Teil davon soziale Medien als festen Bestandteil seiner alltäglichen Kommunikation – bei unverändert steigender Tendenz (z. B. Frees und Koch

2018). Diese Veränderung und Erweiterung grundlegender Interaktionsprozesse auf globaler Ebene bringt zwangsläufig auch negative Begleitphänomene mit sich, die sich u. a. in devianter und delinquenter Form darstellen können – mit all den begrifflichen Schwierigkeiten, die Devianz und Delinquenz in der analogen Welt aufweisen. Ungeachtet dieser Diskussion dürfte es als unbestritten gelten, dass es im virtuellen Raum zu Handlungen kommt, die sowohl in der Allgemeinbevölkerung als auch durch die Strafverfolgungsbehörden mehrheitlich als kriminell eingestuft werden. Beispielhaft sei auf die vielfältigen Formen von Cyberangriffen verwiesen, denen private Internetnutzer/-innen ausgesetzt sind (Dreißigacker et al. 2020) sowie auf die in den letzten Jahren verstärkt diskutierten internetbasierten Anwerbe- und Unterstützungsformen extremistischer und gewaltaffiner, mitunter gar terroristischer Gruppierungen (Nitsch 2020).

Gleichzeitig ist es naheliegend, dass derart gravierende technische und kommunikative Veränderungen sozialer Interaktionsprozesse und -möglichkeiten auch die Gestaltung und das Erleben von Nähe und Beziehungen im sozialen Nahraum verändern: Die Anbahnung und Gestaltung partnerschaftlicher und sexueller Kontakte, das Initiieren und Aufrechterhalten von Freundschaften und Bekanntschaften, aber auch das Austragen (partnerschaftlicher, freundschaftlicher) Konflikte haben sich in den letzten Jahrzehnten verändert und die diesbezüglichen Möglichkeiten wurden erweitert und ergänzt. Bei der Betrachtung und interpretatorischen Einordnung dieser Veränderungen sollten die medientechnischen Entwicklungen jedoch nicht losgelöst von anderen gesellschaftspolitischen Prozessen wie beispielsweise der Individualisierung oder Globalisierung betrachtet werden (Döring 2017). Dies gilt auch für die negativen Effekte der beschriebenen Entwicklungsprozesse, wenn internetbasierte Techniken der Interaktion genutzt werden, um Grenzen zu überschreiten, Menschen zu verletzen oder sexuell, emotional und finanziell auszubeuten. Auch hier kann und sollte die technische Umsetzung der (Straf-)Tat nicht komplett losgelöst von gesamtgesellschaftlichen Phänomenen und den schon seit jeher bekannten individuellen Motiven erfolgen. Gleichzeitig benötigen forensische und kriminologische Theorien und Erkenntnisse wahrscheinlich eine Adaption an den digitalen Raum und sind nicht eins zu eins übertragbar – eine Aufgabe, die bislang noch in ihren Anfängen steckt (Rüdiger und Bayerl 2020).

Eine etablierte kriminologische Theorie, die auch zur Erklärung unterschiedlicher Cyberkriminalitätsformen herangezogen wurde und wird, ist die „Routine-Activity“-Theorie von Cohen und Felson (1979). Die Grundlage dieser Theorie ist das Zusammenspiel zumindest dreier Komponenten für die Erklärung kriminellen Verhaltens: Neben potenziellen Tätern und einem möglichen Zielobjekt muss es an geeigneten Kontrollinstanzen fehlen, die der Tat wirksam

entgegentreten können. Diese Theorie zielt damit besonders auf die Beschreibung von Tatgelegenheitsstrukturen ab und verweist darauf, dass Kriminalität immer auch von Art und Häufigkeit von Täter- und Opferverhalten abhängt. Vor allem routinemäßiges Verhalten erhöht demnach die Risiken für kriminelle Viktimisierungen und kann gleichzeitig Ansätze zur Kriminalprävention bereitstellen. Die Attraktivität der Routine-Activity-Theorie für Erklärungen von Phänomenen im Bereich der Cyberkriminalität ist naheliegend, wenn man – wie zuvor beschrieben – die routinemäßige Durchdringung unseres Alltags durch das Internet bedenkt und daraus die – ebenfalls recht naheliegende – Erklärung ableitet, dass durch diese routinemäßige Internetnutzung vielfältige Tatgelegenheitsstrukturen entstehen.

Ausgehend von dieser theoretischen Überlegung wird deutlich, warum der digitale Raum besonders günstige Tatbegehungsstrukturen aufweist: Zunächst bietet sich ein schier unendlicher sozialer Raum an, in dem potenzielle Opfer kontaktiert werden können, wobei mittels vergleichsweise geringem Aufwand (Versenden einer E-Mail, Erstellen einer Homepage oder das Hochladen einer Bild-, Text- oder Videodatei auf eine bereits existierende Plattform) ein großer Personenkreis erreicht werden kann. Dabei bietet das Internet zumindest auf den ersten Blick simpelste Möglichkeiten der Anonymisierung an, die bei etwas höherem Täterbemühen nur mit hohem Aufwand aufgehoben werden kann. Unter Rückgriff auf die Prämissen der „Rational-Choice“-Theorie (Cornish und Clarke 1986) bietet der digitale Raum somit aus Täterperspektive günstige Ausgangsbedingungen: Einem potenziell hohen Nutzen bzw. Gewinn steht ein vergleichsweise geringes Risiko gegenüber. Durch die sich fortlaufend ändernden technischen Möglichkeiten ist es für die potenziell Betroffenen zudem schwierig, unter den permanent verändernden Gegebenheiten die notwendigen Schutzmaßnahmen vor digitalen Angriffen zu aktualisieren, wodurch technisch versierten Tätern bzw. Tätergruppen laufend neue Tatmöglichkeiten geboten werden.

Zuletzt sei die Rolle der Kontrollinstanzen angesprochen, die zunächst eine – in Anbetracht der riesigen Menge an Normbrüchen nachvollziehbare – Überforderung dahingehend aufweisen, die Sanktionspraxis aufrechtzuerhalten und durchzusetzen. Es ist eine kriminalpolitische Binsenweisheit, dass Kriminalität – nicht nur, aber insbesondere auch die Cyberkriminalität – in einem globalisierten Kontext agiert, während Strafverfolgungsbehörden weiterhin überwiegend innerhalb nationalstaatlicher Grenzen operieren (müssen), wodurch ihre Kompetenzen und Wirkmöglichkeiten eng beschränkt werden. Dies kann jedoch dazu führen, dass normverletzendes Verhalten im digitalen Raum über einen längeren Zeitraum sichtbar bleibt und so den Rezipienten/-innen eine „Normalität“ (im Sinne einer Normkonformität) suggeriert, die im analogen Raum kaum denk-

bar wäre. Wird im öffentlichen Raum ein (schwerwiegender) Gewalt- oder Sexualdelikt begangen, erinnern ggf. für einige Tage Spuren des Verbrechen an den Normbruch; im Internet können Rechtsbrüche mitunter Jahre sichtbar bleiben bzw. immer wieder, teilweise in leicht veränderter Form, auftauchen.

Dieser Effekt, der auch als „fixierte Kriminalitätstransparenz“ (Rüdiger und Bayerl 2020, S. 5) beschrieben wurde, kann zur Folge haben, dass die Normorientierung weiterer Internetnutzer/-innen untergraben und kriminalpräventive Bemühungen im digitalen Raum damit konterkariert werden. Diese exponentiell gesteigerte Wahrnehmbarkeit von Normbrüchen führte in der Vergangenheit mehrfach zur öffentlichen Diskussion darüber, ob das Internet gar als ein „rechtsfreier Raum“ anzusehen sei (Hoheisel-Gruler 2020). Es ist naheliegend, dass derartige Wahrnehmungen geeignet sind, das Vertrauen in Rechtsstaatlichkeit im Allgemeinen sowie in die Schutzmöglichkeiten der Strafverfolgungsbehörden im Besonderen in weiten Teilen der Bevölkerung zu desavouieren.

Neben den reduzierten Zugriffsmöglichkeiten der formalen Sozialkontrolle durch staatliche Instanzen sind in bestimmten digitalen Interaktionsfeldern auch die Möglichkeiten der informellen Sozialkontrolle beschränkt. Dies trifft beispielsweise dort zu, wo aufgrund der Anonymität Personen nicht oder nur bedingt mit ihrem grenzverletzenden Verhalten konfrontiert werden können oder sich leicht einer Konfrontation entziehen können. Auf streng vorselektierte Nutzerkreise beschränkte Foren verhindern bzw. erschweren informelle Sozialkontrolle zusätzlich. Das Phänomen der dauerhaften, scheinbar oder tatsächlich konsequenz- bzw. sanktionslosen Präsenz des Normbruchs kann darüber hinaus für bestimmte Deliktbereiche, wie beispielsweise im Kontext von „Hate-Speech“-Taten oder bei Fällen des Trennungstalkings (s. ausführlicher dazu im Folgenden), sogar zusätzlich tatmotivierend wirken.

Diese theoretische Betrachtung verdeutlicht gleichzeitig, wie aus der Routine-Activity-Theorie Ansatzpunkte für Präventionsbemühungen abgeleitet werden können (Ehlert und Rüdiger 2020). Gemäß den theoretischen Grundannahmen könnte kriminalpräventiv bei den potenziellen Opfern angesetzt werden, indem sie für Übergriffe und Viktimisierungserfahrungen sensibilisiert werden und Gefahren frühzeitig erkennen und so besser abwehren können. Auch kann versucht werden, potenzielle Täter durch die gezielte Vermittlung von Normen auf den jeweiligen Plattformen und Kommunikationswegen von ihrem Normbruch abzuhalten. Auf der Ebene der Kontrollinstanzen kann versucht werden, das Risiko, als Täter ermittelt und strafrechtlich verfolgt zu werden, zu erhöhen, sodass interne Abwägungsprozesse dazu führen, eine Straftat nicht zu begehen.

Cyberkriminalität im Kontext von Partnerschaft, Sexualität und Peerbeziehungen

Der vorliegende Beitrag beschäftigt sich mit Formen der Cyberkriminalität, bei denen Gewalt, Deliktstrukturen, Bedürfnisse und Motive des sozialen (Nah-)Raums digital transformiert werden. Als Gewalt im sozialen Nahraum werden üblicherweise schädigende interpersonale Verhaltensweisen beschrieben, die in sozialen Situationen ausgeübt werden, die bezüglich der beteiligten Personen durch ein besonderes Näheverhältnis (Intimität, „Verhäuslichung“) gekennzeichnet sind (Brandstetter 2009). Die Gewaltformen, die besonders häufig im Bereich des sozialen Nahraums diskutiert werden, umfassen Gewalthandlungen im familiären und im partnerschaftlichen Kontext. Für den vorliegenden Beitrag wird die Sichtweise darüber hinausgehend um all jene Gewalt- und Kriminalitätsformen erweitert, bei denen Sexualität, Partnerschaft(-swünsche und -skonflikte) und Peerbeziehungen eine zentrale Rolle einnehmen. Das Internet besitzt bei den im Folgenden genannten Kriminalitätsphänomenen dahingehend eine entscheidende Funktion, als dass die Anbahnung und Durchführung der Straftat an internetbasierte Technologien geknüpft sind (das Internet als Tatort und/oder Tatmedium).

Gleichzeitig grenzen wir die im Folgenden besprochenen Deliktbereiche von solchen Formen der Cyberkriminalität ab, bei denen die Opferauswahl willkürlich erfolgt und deliktisches Verhalten möglichst breit gestreut wird, ohne persönlich motivierte Auswahlkriterien zu berücksichtigen; Beispiele hierfür wären die vielfältigen Formen des Onlinebetrugs. Auch personalisierte Angriffe, z. B. in Form sog. Hate-Speeches, werden im vorliegenden Beitrag nicht näher berücksichtigt. Zwar handelt es sich dabei in manchen Fällen um eine gezielte und persönlich motivierte Opferauswahl, der weitaus größere Teil erfolgt aber mit dem Ziel einer möglichst breiten Streuung, ohne auf eine konkrete Person oder einen konkreten Personenkreis ausgerichtet zu sein. Zentrales Motiv ist in der Regel eine (pseudo-)politische Mobilisierung, die durch das Anstoßen oder Verbreiten von Ausgrenzungsdiskursen, Einschüchterung und gruppenbezogenem Dominanzgebaren erreicht werden soll (Schmitt 2017). Persönliche psychosoziale Motive stehen hingegen in der Regel nicht im Vordergrund oder spielen bei dieser Form von Übergriffen und Straftaten überhaupt keine Rolle.

Cyberstalking

Wie auch bei der ursprünglichen Form des Stalkings, die keinen expliziten Bezug zum Kommunikationsweg des Stalkingverhaltens spezifiziert, lassen sich auch für den

Bereich des Cyberstalkings unterschiedliche Definitionen finden (für einen Überblick: z. B. Huber 2013; Port 2012). In dem Versuch, die zentralen Aspekte zu berücksichtigen, kann Cyberstalking als absichtliche, wiederholte und unerwünschte Kontaktaufnahme durch computerbasierte Kommunikationstechniken oder die über diese Techniken stattfindende Verunglimpfung, Bloßstellung oder Bedrohung bezeichnet werden, die bei den Betroffenen Angst auslöst (Southwork et al. 2007; deutsche Übersetzung nach Dreßing et al. 2009).

Die unterschiedlichen Definitionen erschweren genaue Forschungen zur Prävalenz des Cyberstalkings; aussagekräftige bzw. repräsentative Studien aus dem deutschsprachigen Raum liegen bislang noch nicht vor (Port 2012). Einigkeit besteht allerdings darin, dass die Bedeutung des Cyberstalkings zunimmt (Dreßing et al. 2009). Im Bereich des Stalkings allgemein wurden in der *Polizeilichen Kriminalstatistik* (PKS; Bundeskriminalamt 2020) im Jahr 2019 im Bereich Nachstellung (Stalking) 18.905 Fälle registriert und damit eine fast unveränderte Zahl im Vergleich zum Jahr zuvor (im Jahr 2018 wurden 18.960 Fälle erfasst). Dabei wurden 15.904 Täter/-innen ermittelt, die gemäß der PKS-Daten mehrheitlich männlich und im mittleren Erwachsenenalter waren und die deutsche Staatsbürgerschaft besaßen. Die Aufklärungsquote lag dabei über 90 % und kann damit als vergleichsweise hoch eingestuft werden.

Eine häufige Form des Cyberstalkings beinhaltet den Identitätsdiebstahl, bei dem personenbezogene Daten des Opfers – zunächst noch ohne dessen Wissen – missbraucht werden, um in seinem Namen gefälschte E-Mails zu versenden oder rufschädigende Nachrichten in Foren und Gästebüchern zu posten (Port 2012). Auch das Bestellen von Waren oder die Anmeldung in Dating-Plattformen sind verbreitete Formen, mit denen den Betroffenen mitunter erheblicher finanzieller und persönlicher Schaden zugefügt werden kann. Andere Erscheinungsformen des Cyberstalkings sind die digitale Verbreitung von privaten Informationen der betroffenen Person sowie die wiederholte und unerwünschte Kontaktierung des Opfers durch Zusenden von E-Mails (oder anderen Nachrichtendiensten), wobei diese zuletzt genannte Form des Cyberstalkings in empirischen Studien – zumindest zu Beginn der Cyberstalkinghandlungen – das mit Abstand häufigste Täterverhalten darstellte (z. B. Belik 2007). Generell erstreckt sich bei einem Großteil der Taten das Stalkingverhalten über mehrere Monate und in zumindest einem Drittel der Fälle sogar über mehrere Jahre, wobei etwa die Hälfte der Betroffenen angab, in der Regel mehrmals täglich Opfer digitaler Übergriffe geworden zu sein. Innerhalb des Tatzeitraums kann es zu Veränderungen im Täterverhalten kommen, sodass beispielsweise die zu Beginn häufig verwendete Kontaktform über E-Mail sukzessive erweitert wird.

Wie aus diesen Informationen zum Tatverhalten ersichtlich werden dürfte, kann Cyberstalking zu erheblichen Belastungen bei den Betroffenen bis hin zu psychischen Störungen und einem deutlich erhöhten Suizidrisiko führen (Dreßing et al. 2009). Wie die zuvor genannte Definition nahelegt, sind ausgeprägte Angstgefühle fester Bestandteil des Cyberstalkings, die sich bei einem großen Teil der Betroffenen zu Angststörungen entwickeln können. Neben erhöhter Ängstlichkeit weisen depressive und traumabezogene Symptome wie stark erhöhte Wachsamkeit und Schreckreaktionen, Nervosität und innere Unruhe sowie Panikattacken eine hohe Prävalenz auf, wobei digitale und analoge Formen des Stalkings offenbar zu vergleichbaren Folgen führen können (Belik 2007; Pathè und Mullen 1997; Port 2012).

Ähnlich wie bei analogen Stalkingformen werden mehr Frauen als Männer Opfer von Cyberstalking. Weitere demografische Merkmale betreffen Alter (es sind mehrheitlich jüngere Personen betroffen) und Familienstand (mehrheitlich werden ledige Betroffene dokumentiert) sowie einen tendenziell höheren Bildungsstand (Belik 2007; Port 2012). Opfertypologien und empirische Analysen von Täter-Opfer-Charakteristika legen nahe, dass bei allen Stalkingformen die Opfergruppe der ehemaligen Intimpartner/-innen die größte Bedeutung aufweist (Mullen et al. 2000). Darüber hinaus können aber auch Personen, die der Täter aus dem (weiteren) Bekanntenkreis kannte oder am Arbeitsplatz kennenlernte, zu Opfern werden (Port 2012). Auch bis dato fremde Personen können zu Opfern werden, wobei bei dieser Gruppe prominente Personen bzw. Personen des öffentlichen Lebens eine besondere Rolle spielen. Aus kriminalpsychologischer Sicht ist dabei allerdings zu bedenken, dass die Annahme der Fremdheit auf den objektiven Tatcharakteristika beruht und die Beziehung von der subjektiven Sichtweise des Täters bzw. der Täterin als bekannt und gar intim und sehr persönlich wahrgenommen werden kann. Der Täter bzw. die Täterin projiziert Beziehungswünsche und -fantasien auf die ihm aus den Medien und vor allem dem Internet bekannte Person, wobei die Tatsache, dass mittlerweile eine große Menge an Bildmaterialien und Informationen über bekannte und prominente Personen im Internet verfügbar ist, das subjektive Gefühl bzw. die Illusion der Vertrautheit und Nähe verstärken kann. Unabhängig von Personen, die aus Film und Fernsehen bekannt sind (Schauspieler, Künstler, Sportler, Politiker etc.) weisen Menschen in exponierten Berufen ein erhöhtes Cyberstalkingrisiko auf – zu dieser Gruppe werden auch Ärzte, Psychologen, Anwälte und Lehrer gezählt (Mullen et al. 2000).

Auf der Täterseite zeigen die demografischen Daten, die überwiegend aus internationalen Studien stammen (für einen Überblick: z. B. Huber 2013; Port 2012), dass die Täter mehrheitlich männlich, im mittleren Erwachsenenalter

und alleinstehend sind sowie häufig über einen höheren Bildungsgrad verfügen. Wenn man die oben genannten Daten der *PKS* damit ins Verhältnis setzt, zeigen sich zumindest hinsichtlich einzelner demografischer Merkmale Parallelen (Alter, Geschlecht), die für eine gewisse Generalisierbarkeit sprechen. Kriminalpsychologisch und forensisch bedeutsam können Überlegungen zu Tätertypologien sein, von denen aus auf Motive, persönlichkeitspsychologische und rückfallrisikobezogene Korrelate geschlossen werden kann. Während für analoge Stalkingformen mittlerweile sehr elaborierte Typologien vorliegen (z. B. MacKenzie et al. 2009), ist die Erkenntnislage bei Cyberstalkern diesbezüglich noch sehr überschaubar. Versucht man die bisherigen tätertypologischen Überlegungen zusammenzuführen (für einen Überblick: z. B. Port 2012), zeigt sich, dass sich ein Idealtypus im Bereich des Trennungs- bzw. Beziehungstalkings abbildet. Ein weiterer Idealtypus wird als wahnhaft beschrieben, da er meist nie Kontakt zum Stalkingopfer hatte, sondern sämtliche (Beziehungs-)Ideen ausschließlich seiner Fantasie entspringen und dort eine zunehmend wahnhaftige Qualität annehmen. Zuletzt wird eine Gruppe von Cyberstalkern beschrieben, die als „rachsüchtig“ charakterisiert werden, weil sie durch ihr Cyberstalkingverhalten versuchen, vermeintliche oder tatsächliche Demütigungen der Vergangenheit, die im Gegensatz zum zuvor genannten Beziehungs- bzw. Trennungstalking nicht zwangsläufig im Kontext von Intimpartnerschaften aufgetreten sind, durch Cyberstalking zu kompensieren.

Cybergrooming

Der Begriff Cybergrooming beschreibt die Anbahnung und Planung von sexuellen Übergriffen im Internet, wobei nach der im deutschsprachigen Raum gemeinhin verwendeten Definition ausschließlich Kinder oder Jugendliche Opfer dieser Handlungen sind bzw. sein können (Böhme 2017). Aufgrund der Tatsache, dass Kinder sich zunehmend mit sozialen Netzwerken oder Online-Multiplayer-Spielen befassen, nehmen auch Tatgelegenheiten zu (Rüdiger 2013; Wolfert und Leven 2019). Die Täter/-innen halten sich in diesen „Social Communities“ auf und täuschen eine Identität vor, deren Lebensumstände denen des Opfers ähneln, wodurch die Wahrscheinlichkeit einer erfolgreichen Kontaktaufnahme erhöht werden soll. Ziele solcher Handlungen sind der Austausch von persönlichen Inhalten und (freizügigen, sexualisierten) Bildern sowie das Führen sexualisierter Kommunikation bis hin zur Anbahnung von persönlichen Treffen, um sexuelle Kontakte zu ermöglichen (Huber 2015). Beim Cybergrooming werden zwei Tätertypen unterschieden: Einerseits gibt es den „Erpresser“, der direkt und offen Kontakt zu den Opfern aufnimmt, um relativ schnell eine sexuell orientierte Kommunikation anzubahnen. An-

dererseits versucht der „indirekte Tätertypus“ zunächst, eine längerfristig ausgerichtete emotionale Bindung zum Opfer aufzubauen, um anschließend das gewonnene Vertrauen zur Befriedigung seiner sexuellen Bedürfnisse auszunutzen (Rüdiger 2013).

Das Cybergrooming zum Nachteil von Kindern (nicht von Jugendlichen) ist gemäß § 176 Abs. 4 Nr. 3 StGB strafbar. Umfasst ist hier seit der Gesetzesänderung am 13.03.2020 nicht mehr nur „das vollendete Einwirken auf ein Kind mit dem Ziel, dieses zu sexuellen Handlungen im Kontakt mit einer anderen Person zu bewegen oder das Kind zum Objekt einer kinderpornographischen Schrift zu machen“ (Dessecker 2019, S. 282), sondern auch der Versuch. Dabei ist ein Anbahnungsverhalten, das sich versehentlich an sog. untaugliche Personen richtet (d. h. kein Kind anspricht, obwohl genau das intendiert war; stattdessen wird ohne Wissen des Täters beispielsweise ein sich als Kind ausgebender Polizeibeamter kontaktiert), nun unter Strafe gestellt.

Die *PKS* zeigt seit 2011 einen stetigen Anstieg der Anzahl von Betroffenen durch Cybergrooming von anfangs 1134 in 2011 auf mittlerweile 2814 Personen im Jahr 2019. Dabei sind etwa drei Viertel der polizeilich registrierten Opfer weiblich. Noch deutlicher stieg die Zahl der Tatverdächtigen von 652 im Jahr 2011 auf 2103 im Jahr 2019 an. Der Anteil weiblicher Tatverdächtiger bewegt sich dabei im einstelligen Bereich (Bundeskriminalamt 2019). Zu diesen Zahlen ist anzumerken, dass davon auszugehen ist, dass derartige Taten nur selten der Polizei gemeldet werden und das Dunkelfeld vergleichsweise groß ausfällt (Böhme 2017; Rüdiger 2013).

Dabei kamen Dunkelfeldstudien zur Häufigkeit von derartigen sexuell motivierten Kontaktversuchen bislang zu sehr unterschiedlichen Ergebnissen und unterschieden sich hinsichtlich der Art der Kontaktaufnahmen (Bergmann und Baier 2016). Eine bereits etwas weiter zurückliegende Studie ermittelte, dass die Hälfte der Schüler/-innen der 5. bis 11. Jahrgangsstufe, die in Chatrooms aktiv waren, über das Internet zu sexueller Kommunikation gedrängt worden sei (Katzer 2008). Außerdem berichteten etwa 10% der Befragten, ihnen sei pornografisches Material geschickt oder sie seien zu sexuellen Handlungen vor der Webcam aufgefordert worden. Bei einer aktuelleren Schülerbefragung der 9. Klassen zeigte sich ebenfalls ein relativ hoher Anteil von 41%, der eine Kommunikation mit unbekanntem Dritten über persönliche, allerdings nicht nur sexuelle Inhalte angab (Bergmann und Baier 2016, S. 182), ca. 13% wurden nach sexuellem Material gefragt und etwa 2% wurden damit erpresst (Bergmann und Baier 2016). Mädchen waren in beiden Studien häufiger Opfer als Jungen (Bergmann und Baier 2016; Katzer 2008). Im Gegensatz dazu ermittelte eine andere Studie aus Deutschland deutlich geringere Prävalenzzahlen: Demnach seien lediglich 4% der 10- bis 18-

Jährigen von anderen Jugendlichen und 3 % von Erwachsenen über das Internet sexuell belästigt worden (Bundesverband Informationswirtschaft Telekommunikation und neue Medien 2014).

Diese Unterschiede bei den ermittelten Prävalenzwerten des Cybergroomings lassen sich zumindest in Teilen auf divergierende Definitionen und Erhebungsmethoden zurückführen und verdeutlichen (erneut), dass einheitlichere Formulierungen wünschenswert wären, um Trends und Studienergebnisse besser interpretieren zu können (Bergmann und Baier 2016). Die Folgen solcher Erlebnisse sind für die Betroffenen ebenfalls relativ unterschiedlich, können jedoch mitunter zu ausgeprägten psychischen Belastungen bis hin zu depressiven Erkrankungen führen (Bergmann und Baier 2016). Auf der Präventionsebene wurden und werden unterschiedliche Maßnahmen diskutiert, die teilweise auch bereits implementiert wurden: So wurden Meldefunktionen in Online-Multiplayer-Spielen etabliert, die allerdings erst relevant werden, nachdem eine Tat stattgefunden hat. Als Antwort auf den weiterhin ansteigenden Trend werden weiterhin die zwingende Implementierung von Kinderschutzmechanismen in derartigen „Social Communities“ sowie kontrollierte Alterseingaben gefordert (Rüdiger 2013).

Zuletzt sei auf eine spezifische Form des Cybergroomings hingewiesen, deren Erforschung noch relativ am Anfang steht, die jedoch gleichzeitig eine hohe kriminologische Relevanz aufweist: Das Cybergrooming als terroristische Taktik zur Rekrutierung von (Ehe-)Frauen für Anhänger des sog. Islamischen Staats (IS). Durch Rückgriff auf das Konzept des Cybergroomings wird ein Perspektivenwechsel vollzogen, durch den der Rekrutierungsprozess nicht als eine professionalisierte Handlungsweise analysiert wird, sondern als Handlungen ideologiegetriebener Täter, die versuchen, ihre Opfer durch einen Vertrauensaufbau im Rahmen eines Groomingprozesses in ein Missbrauchssystem einzubinden (Böttcher 2020). Hierdurch sollen einerseits neue Anhänger/-innen rekrutiert sowie gleichzeitig Geld- und Sachmittel erbeutet werden; dabei weist die Groomingform des Delikts für die Täter/-innen mehrere Vorteile bzw. einen vergleichsweise hohen Nutzen bei zunächst niedrigen Kosten auf.

Cyberbullying

Die Nutzung der Anonymität zur Begehung von Straftaten steht beim Cyberbullying, das auch als Cybermobbing bezeichnet wird, ebenfalls im Mittelpunkt. Hierbei handelt es sich um Mobbinghandlungen (d.h. wiederkehrende psychische Gewalttaten), die geeignet sind, das Ansehen der betroffenen Person zu schädigen und sie psychisch herabsetzen, wobei beim Cybermobbing oder Cyberbullying die Taten über das Internet ausgeführt werden. Sie unterschei-

den sich von herkömmlichen Bullyingformen u. a. dahingehend, dass die handelnden Täter/-innen wechseln können und die Handlungen damit von einer größeren Gruppe von Personen ausgehen, die zumindest teilweise auch anonym bleiben können (Baier et al. 2016; Festl 2015; Schöttker et al. 2018). Ergänzend findet eine räumliche, soziale und zeitliche Entgrenzung statt, da Inhalte öffentlich sowie kontext- und situationsungebunden zugänglich sind und nicht wieder ohne Weiteres gelöscht werden können.

Insgesamt lassen sich bezüglich der Häufigkeit keine genauen Angaben machen, da Fälle von Cybermobbing zum einen nicht zwangsläufig immer strafbar sind und zum anderen im Falle der Strafbarkeit unterschiedliche Straftatbestände erfüllen können. Bei letzterer Tatgruppe kommen beispielsweise Beleidigung (§ 185 StGB), üble Nachrede (§ 186 StGB) oder Verleumdung (§ 187 StGB) in Betracht. Allerdings sind sowohl Opfer als auch Täter/-innen häufig Kinder bzw. Jugendliche, auf die sich auch der Großteil der – deutschen wie auch internationalen – wissenschaftlichen Literatur zum Thema bezieht. Dabei ist dieser Personen-Gruppe die Möglichkeit der Opferwerdung im Netz durchaus bewusst: So stimmten in der sog. Shell-Studie über die Hälfte der 12- bis 25-jährigen Befragten der Aussage zu, dass in sozialen Netzwerken häufig bloßstellende oder verletzende Gehässigkeiten verbreitet werden (Wolfert und Leven 2019). Neuere Dunkelfeldbefragungen in Deutschland bestätigten, dass ein vergleichsweise hoher Anteil von Kindern und Jugendlichen bereits Erfahrungen mit Cyberbullying gemacht hat. So zeigte der sog. Niedersachsensurvey des Kriminologischen Forschungsinstituts Niedersachsen (KFN), dass annähernd die Hälfte der befragten Schüler/-innen der 9. Klasse Cyberbullying innerhalb des letzten Schuljahres erlebt haben, während 5 % angaben, dem sogar regelmäßig ausgesetzt gewesen zu sein (Bergmann et al. 2019). Die Berichte über sexuell motiviertes Cyberbullying sind geringer ausgeprägt; dies wurde von 17–19 % der Befragten innerhalb des vergangenen Schuljahrs erlebt, von etwa 3 % regelmäßig (Bergmann et al. 2019). Der Vergleich zu früheren Schülerbefragungen des KFN zeigt, dass sowohl Täter- als auch Opferzahlen bezüglich des Cyberbullyings eine zunehmende Tendenz aufweisen (Bergmann et al. 2019).

Zu ähnlichen Ergebnissen kam eine Befragung von Schülern der 5., 7. und 10. Klassen an Bonner Schulen, nach der knapp 46 % bereits Erfahrung mit Cybermobbing gemacht hatten (Weber 2018). Deutlich geringere Anteile Betroffener ergab eine weitere Studie aus Deutschland, gemäß der etwa 23 % der befragten Schüler/-innen der Jahrgangsstufen 7 bis 10 Opfer von Cyberbullying geworden sind, wobei sich die Häufigkeiten je nach Art der Cyberbullyinghandlung unterscheiden (Schöttker et al. 2018). Prävalenzunterschiede je nach Art der Handlungen zeigten sich auch in einer Studie des Medienpädagogischen

Forschungsverbands Südwest: Etwa 8% der Kinder und Jugendlichen zwischen 12 bis 19 Jahren gaben hier an, „im Internet fertiggemacht“ (Feierabend et al. 2017, S. 60) worden zu sein; bei über einem Fünftel der Befragten wurden beleidigende oder falsche Inhalte im Netz verbreitet. Aus diesen Ergebnissen wird deutlich, dass die Angaben zur Prävalenz von Cyberbullying je Definition und Art der Messung stark variieren können – ein Befund, der auch in der internationalen Literatur berichtet wird (Porsch und Pieschl 2014).

Von viktimologischer Perspektive aus betrachtet spielen bei der Bewertung der Folgen von Cybermobbing für die Betroffenen die unbegrenzte, kontext- und situationsungebundene Sichtbarkeit der Mobbing- bzw. Bullyinghandlungen im Netz und die dadurch fehlenden Rückzugsmöglichkeiten eine besondere Rolle (Porsch und Pieschl 2014). Die durch das Mobbing entstandenen Belastungen können dadurch besonders schwerwiegend und lang anhaltend sein (Baier et al. 2016; Bergmann et al. 2019; Huber 2015). Insgesamt hängen die Folgen von Cybermobbing von der Art und Intensität sowie der Häufigkeit der Handlungen ab, zudem spielen Resilienzfaktoren (protektive oder Schutzfaktoren) sowie das soziale Umfeld der Betroffenen eine relevante Rolle (Porsch und Pieschl 2014). Aus präventiver Sicht interessant ist die Erkenntnis, dass sowohl Opfer als auch Täter/-innen neben dem digitalen Bullying auch in andere, analoge Bullyingformen involviert waren (Olweus 2012; Porsch und Pieschl 2014).

Scamming

Scamming oder auch Love- oder Romance-Scamming (engl. „scam“: Betrug, Schwindel) ist vergleichbar mit dem Phänomen des Heiratsschwindels, der allerdings auf digitale Interaktionen beschränkt bleibt. Ähnlich wie beim Cybergrooming basieren auch diese Straftaten darauf, zunächst eine Vertrauensbasis aufzubauen und anschließend auszubauen, ohne dabei von Täterseite den Anonymitätsschutz des Internets aufzugeben (Heubrock und Böttcher 2011; Marx und Rüdiger 2017; Treibel 2019).

Mittlerweile werden für die Partnersuche und -vermittlung diverse Portale im Internet angeboten, die auf verschiedene Arten das Ziel verfolgen, Personen bei der Suche nach partnerschaftlichen oder sexuellen Beziehungen zu unterstützen. Auf diesen Portalen können Personen ein Profil anlegen, auf dem sie sich durch persönliche Angaben und Bilder vorstellen und präsentieren. Sie dienen somit primär der Kontaktaufnahme, (anschließend) als Kommunikationsplattform und sind meist der Ausgangspunkt des Romance-Scammings. Dabei handelt es sich um eine spezielle Betrugsart, bei der die Betrüger/-innen zunächst zu Personen Kontakt aufnehmen, die auf der Suche nach ei-

ner Partnerschaft sind. Sie geben anschließend Beziehungsabsichten und -interessen vor, das eigentliche Ziel besteht jedoch darin, später Geldbeträge von den Opfern zu erbeuten (Heubrock und Böttcher 2011; Füllgrabe 2015; Treibel 2019).

Für die erste Kontaktaufnahme werden z. T. auch „Bots“ genutzt, die automatisch Anfragen an eine große Menge von Personen verschicken, sodass die Wahrscheinlichkeit steigt, mit relativ wenig Aufwand ein geeignetes Opfer zu kontaktieren (Heubrock und Böttcher 2011). In anderen Fällen werden gezielt Opfer ausgewählt und ein Fake-Profil erstellt, das möglichst viele Gemeinsamkeiten mit dem Opfer aufweist. In der Regel wird versucht, nach der ersten Kontaktaufnahme möglichst schnell Intimität und eine enge emotionale Beziehung herzustellen, die vergleichsweise früh auch Liebesgeständnisse und das Teilen (angeblich) persönlicher und intimer Informationen beinhaltet (Füllgrabe 2015). Im nächsten Schritt werden dem Opfer finanzielle Notsituationen geschildert, um die Betroffenen dazu zu bringen, größere Geldbeträge zu überweisen: Als Anlässe werden beispielsweise die Krankheit eines Verwandten oder die anstehende Reise des/-r Betrügers/-in zum Opfer benutzt. Der Geldtransfer wird so abgewickelt, dass man ihn nicht bzw. nur schwer nachvollziehen kann, beispielsweise mit Bezahlmodellen wie Paypal oder Western Union (Heubrock und Böttcher 2011; Füllgrabe 2015; Marx und Rüdiger 2017).

Verlässliche Angaben über die Häufigkeit von Scammingtaten in Deutschland gibt es bislang nicht, aber es wird davon ausgegangen, dass es eine der häufigsten und lukrativsten digitalen Betrugsarten ist (Sorell und Whitty 2019). Die Tatsache, dass mittlerweile ein substanzieller Teil der Bemühungen zur Partnersuche durch Portale im Internet erfolgt, hat die Tatgelegenheiten für diese Art der Betrugsdelikte vervielfacht, weshalb eine stetige Zunahme von Opferzahlen und erbeuteten Geldbeträgen zu verzeichnen ist (Sorell und Whitty 2019). Dabei ist zu beachten, dass ein relativ großer Teil dieser Betrugsfälle im Dunkelfeld verbleiben dürfte, da die Betroffenen entweder aus Scham oder aufgrund der Tatsache, dass ihnen die Straftat nicht als solche bewusst wird, keine Anzeige erstatten (Füllgrabe 2015; Treibel 2019).

Bei den Opfern handelt es sich – zumindest in jüngerer Zeit – überwiegend um Frauen (Sorell und Whitty 2019). Die Folgen für die Opfer sind nach solchen Erfahrungen unterschiedlich, können jedoch z. T. massive psychische Belastungen beinhalten. Neben den – teilweise erheblichen – finanziellen Verlusten kann der immense Vertrauensbruch zu weitreichenden psychischen und interpersonalen Problemen führen (Whitty und Buchanan 2015). Zur Prävention vor Romance-Scamming wurden mittlerweile Empfehlungen erarbeitet, nach denen Personen, die eine andere Person im Internet kennengelernt haben, geraten wird, Bilder, Na-

men oder empfangene Texte dahingehend zu prüfen, ob sie bereits zuvor als Scammer/-in aktiv war; dies kann relativ einfach durch die Eingabe des Namens (oder anderer personenbezogener Informationen) in einschlägige Suchmaschine erfolgen (Heubrock und Böttcher 2011).

Fazit

Die Darstellung aktueller cyberkrimineller Ausdrucksformen verdeutlicht, dass dieser Delinquenzbereich zum einen in den letzten Jahren stetig an Bedeutung gewonnen hat, und zeigt zum anderen, dass nach wie vor zentrale Aspekte der genannten Phänomene, deren wissenschaftliche Kenntnis für eine fachliche Auseinandersetzung unumgänglich sind, zumindest bislang nicht ausreichend bekannt sind. Dazu gehören beispielsweise Einigkeit über definitorische Details, die wiederum Voraussetzung für eine vergleichbare Erfassungsmethodik darstellen. Erst dann ist es wiederum möglich, verlässliche und vergleichbare Studien zur Prävalenz, zum Verlauf und zur kriminologischen Entwicklung der Delinquenzbereiche sowie zu zentralen Täter- und Opfermerkmalen durchzuführen. Aufgrund dieses Mangels an verlässlichen Daten und der begründeten Annahme relativ großer Dunkelfelder sind kriminalpräventive Überlegungen derzeit vorrangig auf die Übertragung „klassischer“ Kriminalitätstheorien auf den Bereich der Cyberkriminalität angewiesen. Wer die gesellschaftspolitischen Diskussionen um Digitalisierung verfolgt und die völlige Durchdringung unseres Alltags durch digitale Interaktions- und Kommunikationsformen beobachtet, der muss zwangsläufig zu der Annahme gelangen, dass die Bedeutung der Cyberkriminalität weiter zunehmen wird. Umso wichtiger erscheint eine fachliche Diskussion um Notwendigkeit und Ausgestaltung einer spezifischen Cyberkriminologie dieser digitalen Delinquenzformen.

Funding Open Access funding provided by Projekt DEAL.

Interessenkonflikt M. Rettenberger und F. Leuschner 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

- Baier D, Krenz M, Bergmann MC (2016) Verbreitung und Einflussfaktoren des Cyberbullyings: Ergebnisse einer Repräsentativbefragung in Niedersachsen. *Z Soziol Erzieh Sozialisation* 36:227–245
- Belik C (2007) Cyberstalking – Stalking im Internet, Foren, Newsgroups, Chats, per eMail. Books on Demand GmbH, Norderstedt
- Bergmann MC, Baier D (2016) Erfahrungen von Jugendlichen mit Cybergrooming: Schülerbefragung – Jugenddelinquenz. *Rechtspsychologie* 2:172–189
- Bergmann MC, Kliem S, Krieg Y, Beckmann L (2019) Jugendliche in Niedersachsen. Ergebnisse des Niedersachsensurveys 2017. Kriminologisches Forschungsinstitut Niedersachsen, Hannover
- Böhme G (2017) „Cybergrooming“ – Gefahren in virtuellen Welten und Handlungserfordernisse für die Polizei. *Kriminalistik* 4:269–273
- Böttcher A (2020) Posterboys und Terrorpropaganda: Cybergrooming als terroristische Taktik zur Rekrutierung von (Ehe)Frauen für IS. In: Rüdiger TG, Bayerl PS (Hrsg) *Cyberkriminologie – Kriminologie für das digitale Zeitalter*. Springer VS, Wiesbaden, S 373–396
- Brandstetter M (2009) Gewalt im sozialen Nahraum – Zur Logik von Prävention und Vorsorge in ländlichen Sozialräumen. Springer VS, Wiesbaden
- Bundeskriminalamt (2019) Fälle, Aufklärung, Schaden. Polizeiliche Kriminalstatistik der Bundesrepublik Deutschland: Jahrbuch 2018, Bd. 1. Bundeskriminalamt, Wiesbaden
- Bundeskriminalamt (2020) Polizeiliche Kriminalstatistik 2019: Ausgewählte Zahlen im Überblick. Bundesministerium des Innern, für Bau und Heimat, Berlin
- Bundesverband Informationswirtschaft Telekommunikation und neue Medien (2014) Jung und vernetzt. Kinder und Jugendliche in der digitalen Gesellschaft. Bundesverband Informationswirtschaft, Telekommunikation und neue Medien (BITKOM), Berlin
- Cohen LE, Felson M (1979) Social change and crime rate trends: a routine activity approach. *Am Sociol Rev* 44:588–608
- Cornish D, Clarke R (1986) The reasoning criminal: rational choice perspectives on offending. Springer, New York
- Dessecker A (2019) Zur Diskussion über eine Erweiterung der Strafbarkeit von Cybergrooming. *Kriminalpolit Z* 5:282–286
- Döring N (2017) Sexualität im Digitalzeitalter. *Z Sex-Forsch* 30:1–6
- Dreißigacker A, von Skarczynski B, Bergmann MC, Wollinger GR (2020) Cyberangriffe gegen private Internetnutzer*innen – Gleiches Risiko für alle? In: Rüdiger TG, Bayerl PS (Hrsg) *Cyberkriminologie – Kriminologie für das digitale Zeitalter*. Springer VS, Wiesbaden, S 319–344
- Dreßing H, Klein U, Bailer J, Gass P, Gallas C (2009) Cyberstalking. *Nervenarzt* 80:833–836
- Ehlert C, Rüdiger TG (2020) Defensible Digital Space – Die Übertragbarkeit der Defensible Digital Space Theory auf den digitalen Raum. In: Rüdiger TG, Bayerl PS (Hrsg) *Cyberkriminologie – Kriminologie für das digitale Zeitalter*. Springer VS, Wiesbaden, S 151–171
- Feierabend S, Plankenhorn T, Rathgeb T (2017) JIM 2017. Jugend, Information, (Multi-)Media. Basisstudie zum Medienumgang 12-bis 19-Jähriger in Deutschland. Medienpädagogischer Forschungsverbund Südwest, Stuttgart
- Festl R (2015) Täter im Internet – Eine Analyse individueller und struktureller Erklärungsfaktoren von Cybermobbing im Schulkontext. Springer VS, Wiesbaden
- Frees B, Koch W (2018) ARD/ZDF-Onlinestudie 2018. Zuwachs bei medialer Internetnutzung und Kommunikation. *Media Perspekt* 9:398–413

- Füllgrabe U (2015) Online-Heiratsschwindel und andere Beziehungsfällen. *Kriminalistik* 8–9:487–493
- Heubrock D, Böttcher M-H (2011) „Scamming“ – Betrug durch vorge-täuschte Heiratsabsichten in Internet-Partnerschaftsportalen. *Kriminalistik* 2:75–81
- Hoheisel-Gruler R (2020) Der digitale Raum ist kein (grund-)rechts-freier Raum. In: Rüdiger TG, Bayerl PS (Hrsg) *Cyberkriminalologie – Kriminologie für das digitale Zeitalter*. Springer VS, Wiesbaden, S 71–108
- Huber E (2013) *Cyberstalking und Cybercrime – Kriminalsoziologi-sche Untersuchung zum Cyberstalking-Verhalten der Österrei-cher*. Springer VS, Wiesbaden
- Huber E (2015) Cybercrime gegen Privatpersonen. In: Guzy N, Bir-kel C, Mischkowitz R (Hrsg) *Ziele, Nutzen und Forschungsstand. Viktimisierungsbefragungen in Deutschland, Bd. 1. Bundeskrimi-nalamt, Wiesbaden*, S 393–420
- Katzer C (2008) Cyberbullying und sexuelle Viktimisierung von Kindern und Jugendlichen in Chatrooms. *Forum Kriminalprä-v* 3:26–33
- MacKenzie RD, McEwan TE, Pathé MT, James DV, Ogloff JRP, Mul-len PE (2009) Stalking – Ein Leitfaden zur Risikobewertung von Stalkern: Das „Stalking Risk Profile“. Kohlhammer, Stuttgart
- Marx K, Rüdiger TG (2017) Romancescamming: Eine kriminologisch-linguistische Betrachtung. *Kriminalistik* 4:211–218
- Mullen PE, Pathé MT, Purcell R (2000) *Stalkers and their victims*. Cambridge University Press, Cambridge
- Nitsch H (2020) Terrorismus und die Nutzung des Internet. In: Rüdiger TG, Bayerl PS (Hrsg) *Cyberkriminalologie – Kriminologie für das digitale Zeitalter*. Springer VS, Wiesbaden, S 193–216
- Olweus D (2012) Cyberbullying: an overrated phenomenon? *Eur J Dev Psychol* 9:520–538
- Pathé MT, Mullen PE (1997) The impact of stalkers on their victims. *Br J Psychiatry* 170:12–17
- Porsch T, Pieschl S (2014) Cybermobbing unter deutschen Schülerin-nen und Schülern: Eine repräsentative Studie zu Prävalenz, Fol-gen und Risikofaktoren. *Diskurs Kindh Jugendforsch* 1:7–22
- Port V (2012) *Cyberstalking*. Logos, Berlin
- Rüdiger TG (2013) *Sexualtäter in virtuellen Welten*. Oranienburger Schriften, Sonderausgabe, S 9–30
- Rüdiger TG, Bayerl PS (2020) Cyberkriminalologie – Braucht die Kriminologie ein digitales Upgrade? In: Rüdiger TG, Bayerl PS (Hrsg) *Cyberkriminalologie – Kriminologie für das digitale Zeitalter*. Springer VS, Wiesbaden, S 3–12
- Schmitt JB (2017) Online Hate Speech: Definition und Verbreitungsmotivationen aus psychologischer Perspektive. In: Kaspar K, Grä-ber L, Riffi A (Hrsg) *Online Hate Speech. Perspektiven auf eine neue Form des Hasses, Bd. 4. kopaed, Düsseldorf*, S 51–56
- Schöttker R, Körtge S, Käser U (2018) Im Netz verletzt – Schüler- und Lehrerreaktionen auf Cyberbullying. *Bild Erziehung* 71:65–87
- Sorell T, Whitty M (2019) Online romance scams and victimhood. *Secur J* 32:342–361
- Southwork C, Finn J, Dawson S, Fraser C, Tucker S (2007) Intima-te partner violence, technology and stalking. *Violence Against Women* 13:842–856
- Treibel A (2019) Soziale Isolation statt Liebe [Kriminologischer Bei-trag]. *Forens Psychiatr Psychol Kriminol* 13:96–98
- Weber J (2018) *Cybermobbing – wenn neue Medien fertigmachen. Ei-ne Untersuchung zum Cybermobbing im Stadtgebiet Bonn*. LIT, Berlin
- Whitty MT, Buchanan T (2015) The online dating romance scam: the psychological impact on victims—both financial and non-financi-al. *Criminol Crim Justice* 16:176–194
- Wolfert S, Leven I (2019) Freizeitgestaltung und Internetnutzung: Wie Online und Offline ineinandergreifen. In: Albert M, Hur-relmann K, Quenzel G (Hrsg) *18. Shell Jugendstudie: Jugend 2019 – Eine Generation meldet sich zu Wort*. Belz, Weinheim, S 213–246