Cyberkriminologie – Theorien, Methoden, Erscheinungsformen

Reihe herausgegeben von

Thomas-Gabriel Rüdiger, Institut für Cyberkriminologie, Hochschule der Polizei des Landes Brandenburg, Oranienburg, Deutschland

P. Saskia Bayerl, CENTRIC, Sheffield Hallam University, Sheffield, UK

Die Cyberkriminologie versteht sich als ein junger interdisziplinärer Wissenschaftszweig, der Erkenntnisse der Kriminologie, der Sozial-, Rechts- und Polizeiwissenschaften mit den Besonderheiten eines globalen digitalen Kriminalitätsraums kombiniert. Forschungsfelder der Cyberkriminologie sind dabei abweichende Verhaltensweisen und deren Kontrollmöglichkeiten sowie die Entstehung von Normen und Normenbruch im und mit dem digitalen Raum.

Die Cyberkriminologie ist im deutschsprachigen Raum noch wenig etabliert und verankert. So fehlt es an eigenen Lehrstühlen und vor allem an fachspezifischen Publikationen.

Die Reihe „Cyberkriminologie – Theorien, Methoden, Erscheinungsformen" bietet einen fachlichen Rahmen, um eine strategische Entwicklung der Cyberkriminologie als Wissenschaft voranzutreiben. In ihr erhalten Autoren aus allen relevanten Themenbereichen die Möglichkeit, ihre Publikationen in dieser Reihe zu veröffentlichen, methodische Ansätze zur Untersuchung des Forschungsfeldes zu diskutieren und systematische Begriffsauseinandersetzungen und klar strukturierte phänomenspezifische Beschreibungen zu liefern.

Thomas-Gabriel Rüdiger • P. Saskia Bayerl
Hrsg.

Handbuch Cyberkriminologie 2

Phänomene und Auswirkungen

mit 61 Abbildungen und 24 Tabellen

Springer VS

Hrsg.
Thomas-Gabriel Rüdiger
Institut für Cyberkriminologie
Hochschule der Polizei des Landes Brandenburg
Oranienburg, Deutschland

P. Saskia Bayerl
CENTRIC
Sheffield Hallam University
Sheffield, UK

ISSN 2730-9436 ISSN 2730-9444 (electronic)
Cyberkriminologie – Theorien, Methoden, Erscheinungsformen
ISBN 978-3-658-35441-1 ISBN 978-3-658-35442-8 (eBook)
https://doi.org/10.1007/978-3-658-35442-8

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über https://portal.dnb.de abrufbar.

Planung/Lektorat: Cori Antonia Mackrodt
Springer VS ist ein Imprint der eingetragenen Gesellschaft Springer Fachmedien Wiesbaden GmbH und ist ein Teil von Springer Nature.
Die Anschrift der Gesellschaft ist: Abraham-Lincoln-Str. 46, 65189 Wiesbaden, Germany

Das Papier dieses Produkts ist recyclebar.

Einführung zum Handbuch Cyberkriminologie – Band 1 und 2: Momentaufnahme und Einladung zur Fortentwicklung

Prolog

Ein Handbuch der Cyberkriminologie ist auch im Jahr 2023 noch immer ein ambitiöses Unterfangen. Einerseits weil die Cyberkriminologie als Disziplin im deutschsprachigen Raum noch immer im Geburtsprozess steht, auch wenn mit der Gründung des Instituts für Cyberkriminologie an der Hochschule der Polizei des Landes Brandenburg im Jahr 2021 und der Durchführung der ersten Konferenz der Cyberkriminologie eine erste institutionelle Verankerung erfolgt ist (HpolBB, 2021). Andererseits ist das Forschungsfeld als solches noch jung und bleiben viele Forschungsfragen unbearbeitet oder werden vermutlich noch gar nicht gestellt. Dies liegt sicherlich auch daran, dass das Untersuchungsfeld so dynamisch ist, wie wenig andere gesellschaftlichen Prozesse. Der digitale und soziale Kontext ändert sich unaufhörlich, entwickelt und breitet sich aus (Rüdiger & Bayerl, 2020). Neue Technologien und Entwicklungen sind aber nicht nur ein Selbstzweck für eine neue wissenschaftliche Betrachtung oder eine Art Muskelspiel von IT-Firmen, um zu zeigen, wie die digitale Gesellschaft des 21. Jahrhunderts aussehen kann, oder um den neuen großen Technikwurf nach dem Smartphone zu landen. Die Entwicklungen haben vielmehr konkrete Auswirkungen auf fast alle gesellschaftlichen Bereiche. Sie ändern, wie wir arbeiten, konsumieren, unsere Beziehungen knüpfen, Informationen gewinnen, unsere Freizeit verbringen, Jobs und Datingpartner suchen usw.

Annähernd jedes Jahr geraten neue – oder als neu wahrgenommene – technische und digitale Entwicklungen in den Fokus der gesellschaftlichen Betrachtung. Im Jahr 2021 veröffentlichte Mark Zuckerberg seine Vision von einer neuen Generation von Metaversen, d. h. digitalen Welten, in denen man mit Avataren, d. h. virtuellen StellvertreterInnen, interagiert. Passend benannte er sein Unternehmen gleich in „Meta“ um (Meta, 2021). Dabei ist die Vision eines Metaverse, in dem sich Menschen auf der ganzen Welt vernetzen und miteinander über Avatare interagieren, kommunizieren und spielen, alles andere als neu. *Second Life* von Linden Labs, das bereits 2003 entstand, löste mit einem vergleichbaren Konzept vor fast 20 Jahren bereits einen der ersten großen digitalen Hypes aus (Wiley, 2007). Und bereits 2022 wurde die gesellschaftliche Diskussion über die Metaversen 2.0 weitestgehend abgelöst; einerseits durch die rasante Entwicklung von „Deepfake“-Technologien

und deren Auswirkungen (MDR, 2022), andererseits durch die für NutzerInnen sichtbaren Entwicklungen von anwendbaren Formen künstlicher Intelligenzen, wobei hier neben sog. Text-zu-Bild Generatoren sicherlich die Anwendung „ChatGPT“ im Fokus der Betrachtung steht (Deutscher Bundestag, 2023).

Nur um die kriminologische oder auch polizeiliche Relevanz kurz zu zeigen einige Beispiele. Die japanischen Forscher Takagi und Nishimoto haben in einem Experiment gezeigt, dass sie über Stable Diffusion anhand von Gehirnaktivitäten Bilder rekonstruieren können, die sich die ProbantInnen angeschaut hatten (Takagi & Nishimoto, 2023). Entwickelt sich hier eine Möglichkeit, dass in der Zukunft bei polizeilichen Vernehmungen die Vernommenen nur noch an den Tattag denken müssen und dieser wird bildlich dargestellt? Was ist, wenn das gegen den Wunsch der Betroffenen passiert, beispielsweise auch in Unrechtsstaaten? Ist dies dann das Ende von „die Gedanken sind frei“?

Nicht nur die Text-zu-Bild Generatoren haben in kürzester Zeit ihre kriminologische Relevanz gezeigt. Die in den Internetbrowser Bing integrierte Version von ChatGPT soll in Diskussionen mit NutzerInnen schon mehrmals auch dunkle Seiten von sich gezeigt haben. So gab es Medienberichte über Bedrohungen und Beleidigungen durch den Chatbot (Handelsblatt, 2023; Herz, 2023); ein Phänomen, dass bereits bei dem Chatbot „Tay“ von Microsoft im Jahr 2016 aufgetreten ist. Dieser sollte von Twitter-NutzerInnen Sprache lernen und fiel bereits nach kurzer Zeit mit rassistischen Aussagen auf (Beuth, 2016). Wird irgendwann hier die Situation eintreten, dass im digitalen Raum Bots Handlungen begehen, die bei einem Menschen eine Straftat darstellen würden, und für die PolizistInnen nicht mehr unterscheidbar werden von Aussagen echter Menschen? Könnte dann die Polizei auf den Gedanken kommen, eigene Polizeibots bzw. Polizei KIs zu nutzen, um im digitalen Raum eigenständig Streife zu fahren und diesen Mechanismen zu begegnen? Werden wir also irgendwann eine Situation erleben, bei dem sowohl der Normenbruch als auch die Normenkontrolle durch Künstliche Intelligenzen (KI) begangen werden, wir also als eine Art „Entmenschlichung digitaler Kriminalität“ haben? Diese Liste ließe sich vermutlich fast beliebig um digitale Entwicklungen der letzten 20–30 Jahre erweitern. Aus einem kriminalwissenschaftlichen Blickwinkel heraus, haben aber annähernd alle diese Entwicklungen stets auch das Potenzial, Auswirkungen sowohl auf die Kriminalitätsbegehung als auch auf Kriminalitätskontrolle zu entfalten.

Die Kriminologie als die ‚Lehre vom Verbrechen‘ sollte auf solche Entwicklungen theoretisch, methodisch und empirisch reagieren, wenn sie relevant bleiben und auch eine Basis für evidenzbasierte kriminalpolitische Reaktionen bieten möchte. Dies gilt auch, um unreflektierte kriminalpolitische Überreaktionen durch empirische Erkenntnisse zu vermeiden, wie sie beispielsweise im Rahmen der Reform des § 184b StGB zu einem Verbrechenstatbestand diskutiert wird (Bongen & Moßbrucker, 2023; Meister, 2022). Bestehende Theorien müssen geprüft und angepasst und neue methodische Ansätze entwickelt werden, um auch neue digitale Umgebungen, von sozialen Medien und Onlinegames zu Metaversen und Formen des Darknets, sowie sich wandelnde Kapazitäten – Künstliche Intelligenz, Internet of Things, die Vernetzung bzw. ‚Mobilisierung‘ von Daten durch Dronen, Sensoren in Alltags-

gegenständen wie Kleidung oder SmartWatches, Sensoren für Geräusche, Gerüche, Massenverhalten, etc. im Rahmen von Smart Cities, usw. – beschreiben und verstehen zu können.

Dabei steht die Erkenntnis im Mittelpunkt, dass mit dem Internet und digitalen Mechanismen nicht einfach nur neue technische Entwicklungen vorliegen, sondern dass sich mit dem digitalen Raum eine global umspannende Interaktions- und Kommunikationssphäre ohne physisch wahrnehmbare Grenzen gebildet hat. Eine der Besonderheiten dieser Entwicklungen ist, dass Menschen auf der gesamten Welt fast zeitgleich mit denselben digitalen Phänomenen und auch digitalen Kriminalitätsformen konfrontiert werden können (Rüdiger, 2023). Beispielsweise interagieren Menschen von unterschiedlichen Staaten in einem gemeinsamen Metaversum miteinander, werden mit den gleichen Deepfake-Medien konfrontiert oder kommunizieren mit demselben Chatbot. Dabei befinden sich die Menschen physisch aber in ihren eigenen Ländern und unterliegen damit auch dem dortigen Verständnis von Normenbruch und Normenkontrolle (Rüdiger & Bayerl, 2020). Wie genau das Miteinander von Menschen in diesem globalen Raum strukturiert werden soll, ist noch weitestgehend unklar und wird erstaunlich wenig thematisiert.

An diesem Grundverständnis will die Cyberkriminologie ansetzen. Ihr Ziel ist einerseits die Übertragung und Anpassung bisheriger kriminologischer Betrachtungen auf diesen globalen digitalen Raum. Andererseits eröffnen aber die Besonderheiten des digitalen Raums – z. B. die Möglichkeit der massenhaft privaten Kommunikation, einer besonderen digitalen Kriminalitätstransparenz und einer Fixierung von Kriminalität im digitalen Raum, aber auch das Aufeinandertreffen strafrechtlicher Vorstellungen aller Länder – die Entwicklung neuer eigenständiger Erklärungsansätze für digitale Normenbrüche (Rüdiger, 2021). Daher lässt sich die Cyberkriminologie in Anlehnung an die ‚klassische' Definition der Kriminologie, verkürzt am ehesten als die *„Lehre vom digitalen Verbrechen"* definieren oder etwas differenzierter als, *„die Lehre vom Verbrechen, das online oder über digitale Möglichkeiten stattfindet"*.

Neben der namensgebenden Lehre – mit einem Fokus auf Wissensvermittlung, Erkundung und Ursachenerklärung – ist es den Herausgebern dieses Handbuchs allerdings auch wichtig, die Cyberkriminologie als praxis- und lösungsorientiert zu positionieren. Das bedeutet, dass wir speziell Entwicklungen von Maßnahmen für die Erkennung, Ermittlung und Prävention von Straftaten sowie der Täter- und Opferwerdung als Kernbereich dieser Disziplin ansehen. Ein besonderes Interesse liegt demgemäß – neben der Betrachtung und Analyse für Kriminalitätsentwicklungen – auch auf der Frage, welche strafrechtlichen Normen in einem globalen digitalen Raum gelten sollen, wer diese überhaupt bestimmt und wie dann der Bruch dieser Regeln verfolgt und geahndet werden kann. Entsprechend erfasst die Cyberkriminologie aus unserer Sicht auch alle Fragen der digitalen Polizeiarbeit und der Digitalisierung von Prozessen der Sicherheitsbehörden. Von Bedeutung erscheinen hier vor allem die Schaffung der rechtlichen Rahmenbedingungen und organisationalen Voraussetzungen wie Ressourcen, Strukturen, Methoden und Training sowie Fragen der institutionellen Selbstreflexion.

Nachdem im Rahmen des Sammelbandes „Cyberkriminologie“ bereits 2020 ein erster Aufschlag zur konzeptionellen Verankerung durch eine Vielzahl von AutorInnen und Autorenteams aus den unterschiedlichsten Fachdisziplinen vorgelegt wurde, soll diese Entwicklung nun in diesem Handbuch fortgesetzt werden. Dabei soll versucht werden, der unterschiedlichen Themenvielfalt in zwei Bänden gerecht zu werden.

Band 1: Theorien und Methoden

Band 1 bietet einen Überblick über relevante theoretische und methodische Ansätze. Dies sind zum einen wichtige Anpassungen und Erneuerungen bestehender Modelle und Praktiken, zum anderen die Herausbildung neuer Ansätze, mit dem Ziel, den ‚Werkzeugkasten‘ für Akademiker und Praktiker entscheidend zu bereichern und den Betrachtungswinkel zu verbreitern. Der erste Band ist hierfür in die drei Teile unterteilt: (1) Theorien, (2) Methoden und (3) rechtliche Grundlagen.

Der Beitrag „Cyberkriminologie – Kriminologische Ansätze für eine digitale Weltgesellschaft“ von Rüdiger eröffnet die theoretische Betrachtung und führt in die Cyberkriminologie als Disziplin ein, indem u. a. die Broken Web Theorie und das Konzept der digitalen Kriminalitätstransparenz vorgestellt und erörtert werden. Bei beiden Ansätzen steht die Frage im Mittelpunkt, warum der digitale Raum offenbar als teilweise strafverfolgungsfrei wahrgenommen wird und warum die Strafverfolgungswahrscheinlichkeit bei digitalen Delikten tatsächlich niedriger ist als bei analogen Delikten. Acker sieht in seinem Beitrag zur „White Gloves Theory“ ebenfalls das Problem, dass bisherige kriminologische Ansätze, die für das „analoge Leben entwickelt wurden“, Handlungen im digitalen Raum unzureichend berücksichtigen und dieser daher eine besondere Betrachtung erfordert. Die namensgebenden „Gloves“ stellen hierbei eine Metapher dar sowohl für die geringe Wahrscheinlichkeit einer Strafverfolgung als auch für eine digitale Tatbegehung, die für das Umfeld weitestgehend verborgen ist. Das kriminalwissenschaftliche „Spuren- und Indizienparadigma“ in Bezug auf von Cyberkriminalistiken steht anschließend im gleichlautenden Beitrag von Plank und Fiedler im Mittelpunkt der Erörterung. Hierbei zeigen die Autoren, wie die bisherige kriminalistische Handlungslehre und Spurenkunde auch im digitalen Zeitalter ihre Anwendung finden können.

Stefanopoulou greift in ihrem Beitrag die Frage auf, inwiefern „das digitale Netz als soziales System und als kriminologisch relevante Makrostruktur“ betrachtet werden kann. Hierbei verwendet sie ganz in der Tradition des berühmten Soziologen Niklas Luhmann einen systemtheoretischen Blickwinkel auf das digitale Netz. Eine Erkenntnis ist dabei, dass sich Regulierungsdefizite nicht alleine auf individuelles Verhalten beziehen können, sondern auch ein übergeordneter Blick erfolgen muss. Digitale Kriminalität findet dabei nicht nur im Darknet oder auf geheimen Plattformen statt. Kattenberg diskutiert in seinem Beitrag einerseits, dass auch „Soziale Medien kriminogene Orte“ darstellen und andererseits, was unter dem Begriff der „digitalen Resilienz“ anhand des Phänomens „Cybergrooming“ verstanden werden kann. Dabei steht im Mittelpunkt der Online Disinhibition Effect – also eine

Enthemmung in der Onlinekommunikation, ein Umstand der u. a. in Deutschland zur Einführung des Netzwerkdurchsetzungsgesetz (NetzDG) beigetragen haben dürfte. Welche Herausforderungen sich der Polizei bei der Aufgabenerfüllung in soziale Medien stellen, ist Inhalt des Beitrages von Grassl. Dieser beschäftigt sich dabei aus einer kommunikationswissenschaftlichen Perspektive u. a. mit den Auswirkungen von „Hate Speech, Influencern und Medienkompetenz" für die Polizeiarbeit. Grassl kommt hierbei zu der Erkenntnis, dass eine rein „Symptom-bekämpfende Anpassung der polizeilichen Social-Media-Arbeit" nicht den Anforderungen gerecht wird.

Daschmann und Herden eröffnen mit ihrem Beitrag zu „Erhebungs- und Analysemethoden der zukunftsorientierten Polizeiarbeit für die Zwecke der (kommunalen) Kriminalprävention" Teil 2 des ersten Bandes zu „Methoden". Im Rahmen des Beitrags wird aufgezeigt wie vorhandene polizeiliche Daten am Beispiel des Landes Hessen analysiert und für die kommunale Kriminalprävention genutzt werden können. Der zweite Beitrag in diesem Abschnitt von Demus et al. stellt sich der Frage, wie digitale Hasskriminalität definiert und erkannt werden kann. In ihrem Beitrag „Hass im Netz – Aggressivität und Toxizität von Hasskommentaren und Postings, Detektion und Analyse" beschreiben sie, wie sich Hasskriminalität im Netz ausbreitet und wie entsprechende Beiträge identifiziert werden können. Im Mittelpunkt steht dabei die Frage, welche Schlussfolgerungen für Monitoring- und Eindämmungsmaßnahmen gezogen werden können. Ein spannender Ansatz ist dabei der Vorschlag des Autorenteams, dass NutzerInnen „neben Empfehlungen ähnlicher Inhalte gezielt gegensätzliche Ansichten angezeigt werden".

Farthofer diskutiert mit ihrem Beitrag zum „Einsatz von Künstlicher Intelligenz in der Kriminalprävention" die Herausforderungen Künstlicher Intelligenz in der präventiven Polizeiarbeit. Der Fokus liegt hierbei auf Systemen zur geografischen Tatortvorhersage und individuellen Täterbewertung, die in Deutschland und anderen Ländern zum Einsatz kommen. Dabei werden die jeweiligen Vorteile, aber auch die damit verbundenen Probleme näher beleuchtet. Um den möglichen Vorteilen von KI für Polizeiarbeit gerecht zu werden, verlangt die Autorin die Schaffung von gesetzlichen Grundlagen des Einsatzes von KI als die wichtigste Voraussetzung, um vor allem „diskriminierende Auswüchse wie sie in den USA in der letzten Zeit immer wieder festgestellt werden" zu vermeiden.

Zu einem vergleichbaren Ergebnis kommt Ruppert im Rahmen seines Beitrags, der die Frage der Auswertung von großen Datenmengen sog. „Big Data" und die Nutzung von „Algorithmen im Rahmen der Kriminalitätsbegegnung" sowie deren kriminologischen Hintergründe erörtert. Ruppert sieht die Möglichkeit, aus den gewonnenen Informationen durch Ableitungen auch Erkenntnisse und Schlussfolgerungen für die kriminologische Betrachtung zu gewinnen.

„Eine methodische und operative Bewertung" von sog. Predictive Policing Ansätzen bei der belgischen Polizei wird durch die Autoren Hardyns und Klima in ihrem Beitrag vorgenommen. Die Autoren haben dabei seit 2015 den Einsatz von entsprechenden Vorhersagemodellen bei unterschiedlichen „belgischen Polizeizonen" getestet. Dabei kommen sie zu dem Ergebnis, dass es einerseits weitere Forschungen braucht, um eine fundierte Aussage zu treffen, und schlagen anderer-

seits vor, dass man Erfahrungen auch aus anderen Fachdisziplinen – wie beispielsweise der Geografie – heranziehen sollte.

Tatsächlich steht in dem anschließenden Beitrag von Povalej und Volkman im Mittelpunkt, welchen Einfluss datenbasierte Geoinformationssysteme (GIS) und das Building Information Modeling (BIM) auf die Polizeiarbeit haben können. Eine Entwicklung, die früher eher aus Science-Fiction-Filmen bekannt war, wenn Tat- oder Einsatzorte für die Polizei in verschiedenen Dimensionen am Computer oder gar einer Virtual oder Augmented Reality-Brille angezeigt und mit geografischen Informationen kombiniert wurden. Die Autoren beschreiben dabei verschiedene Anwendungsfälle von der Darstellung virtueller Objekte an Tatorten zu täterorientierten Mobilitätsanalysen und Bereichen der Verkehrsunfallaufnahmen. Dabei kommen sie zu der Schlussfolgerung, dass sowohl GIS als auch BIM-Modelle sich als ein dauerhafter Bestandteil einer digitalen Polizeiarbeit etablieren werden.

Die Kriminologie kennt für den analogen Raum unterschiedliche Methoden, um sozial abweichende Verhaltensweisen zu erforschen. Neben klassischen Vorgehensweisen wie Umfragen, Erhebungen oder der Auswertung von Kriminalstatistiken versprechen vor allem qualitative Erhebungsmethoden wie Interviews, (teilnehmende) Beobachtungen und ethnografische Ansätze spannende Erkenntnisgewinne. Diese besitzen allerdings im Rahmen kriminologischer Forschung auch Nachteile. Zum einen sind diese Methoden meist zeit- und ressourcenaufwendig, zum anderen kann ein Risiko für die WissenschaftlerInnen bestehen, wenn diese z. B. im Rahmen der teilnehmenden Beobachtung mit Kriminalität bzw. TäterInnen konfrontiert werden.

Gerstner und van Sintemaartensdijk legen vor diesem Hintergrund einen methodischen Ansatz vor, der die „Erforschung von Kriminalität mit Experimenten in der virtuellen Realität“ ermöglicht; ein verblüffend nahe liegender Ansatz, wenn man die gesellschaftliche Diskussion um Metaversen betrachtet. Die Autoren zeigen dabei auf, wie Virtual Reality die Möglichkeit bietet, VersuchsteilnehmerInnen direkt bei Handlungen und ihren Reaktionen in realitätsnahen Situationen zu beobachten. Gerade der Aspekt der Immersion – also des Gefühls in der jeweiligen virtuellen Welt zu versinken – wird hier eine besondere Bedeutung beigemessen. Als Illustration beschreiben die Autoren ein Experiment bei dem verurteilte Einbrecher aus den Niederlanden und eine Vergleichsgruppe von Studierenden sich durch die VR-Simulation einer Wohngegend bewegen und dabei u. a. auskundschaften, ob die Umgebung für einen Einbruch in Frage käme. Damit können die Autoren sehr detailliert das Potenzial Virtueller Reality und Metaversen für die kriminologische Betrachtung aufzeigen.

Metaverse stehen auch im Mittelpunkt des Beitrags von Pfeiffer et al. zu „Blockchains, Kryptowährungen, Utility-Token, NFTs und das Metaverse“. Der Beitrag soll dabei die Begrifflichkeiten für den Bereich der Cyberkriminologie einführen und beschreiben. Der Schwerpunkt wird hierbei auf die Potenziale wie auch Risiken – vor allem im Bereich der Vermögensdelikte – von Blockchain-basierter Technologie und sog. Non-Fungible Tokens (NFT) gelegt. Hierbei spielen nicht nur Metaversen 2.0 eine Rolle; das Autorenteam setzt sich auch mit dem Einfluss auf den Bereich Social Media auseinander. Dabei kommen sie zu der Schlussfolgerung, dass gerade

Blockchain-Systeme das Potenzial beinhalten, „Cybersecurity-Risiken" zu minimieren, während sie gleichzeitig durch die großen dahinterstehenden Vermögenswerte an Attraktivität für kriminelle Aktivitäten gewinnen.

Metaversen unterscheiden sich von Onlinegames vor allem dadurch, dass bei Letzteren ein spielerischer Kontext überwiegt. Können spielerische Ansätze (sog. Gamification) und das Wissen der „Masse" (sog. Crowdsourcing) auch sinnvoll in der Verbrechensbekämpfung eingesetzt werden? Diesem spannenden Ansatz geht Fenner in ihrem Beitrag nach. Dabei beschreibt die Autorin die Idee, dass NutzerInnen von digitalen Räumen die Arbeit des Rechtsstaats sinnvoll unterstützen können. Der Schwerpunkt des Beitrags liegt in der Verknüpfung beider Ansätze und deren Einsatzmöglichkeiten zur Verbrechensbekämpfung. Die Autorin sieht in beiden Verfahren zukunftstragende Methoden.

Der dritte Teil des ersten Bands umfasst primär rechtliche Fragestellungen im Kontext der Cyberkriminologie, was sowohl Strafrecht, Polizeirecht als auch artverwandte Rechtsgebiete umfasst. Haider betrachtet hierbei die neuen Anforderungen an eine „Strafverteidigung im digitalen Zeitalter", daneben aus der Betrachtung des deutschen Strafrechts Strafbarkeitsfallen und illustrativ das Phänomen des Drogenhandels in Sozialen Medien. Dabei zeigt sie klar auf, dass der digitale Raum nicht nur Herausforderungen für die Seite der Strafverfolgung aufweist, sondern auch für die Einhaltung der „Grundrechte und Verfahrensrechte (von) Cyber-Tätern".

Die Perspektive der Sicherheitsbehörden und der Strafverfolgung nimmt Kunze hingegen mit seinem Beitrag zur „Bearbeitung von Cyberangriffen unter Berücksichtigung der polizeilichen Vorschriftenlage und fachliche, technische und rechtliche Determinanten erfolgreicher Cyberoperationen gegen angreifende Infrastrukturen und Tätergruppierungen (Hack Back)" ein. Der Autor untersucht die unterschiedlichen rechtlichen Landespolizeiinstrumente in NRW, die Reaktionen auf sog. „Ransomware"-Angriffe regulieren. Er kommt dabei zu dem Ergebnis, dass das immer wieder in der Politik geforderte Instrument des „Hack Back" gegenwärtig nicht nur faktisch kaum umsetzbar ist, sondern es zudem sowohl an „nationalen als auch völkerrechtlichen Grundlagen" fehlen würde. Gerade die Frage der Anwendbarkeit gefahrenabwehrrechtlicher Regelungen im digitalen Raum ist dabei in der Wissenschaft, aber auch der Kriminalpolitik ein gering bis kaum diskutiertes Anwendungsfeld (Krischok, 2018). Dabei ist der primäre Gedanke einer polizeilichen Gefahrenabwehr, Menschen vor Straftaten und anderen Formen von Gefahren zu beschützen, bevor diese negativen Konsequenzen haben können, und Gefahren bestmöglich zu verhüten. In der gesellschaftlichen und kriminalpolitischen Betrachtung überwiegt jedoch offenbar die Strafverfolgung, die aber spätestens in einem globalen digitalen Raum an ihre nationalen Grenzen sowohl rechtlicher als auch faktischer Natur stößt. Entsprechend werden auch neue Formen der Normenkontrolle im digitalen Raum ausprobiert.

Eine durchaus in der gesellschaftlichen Kritik stehende Form war bzw. ist das NetzDG. In „Hasskriminalität und Strafverfolgung im Kontext der Novellierung des NetzDG" greift Bone-Winkel dieses Thema in seinem Beitrag auf. Neben einer Analyse der bisherigen Entwicklung von Hasspostings und einer Einschätzung der Wirksamkeit bisheriger kriminalpolitischer Bekämpfungsmechanismen inklusive

dem NetzDG, steht vor allem die geplante Anzeigepflicht von schweren Straftaten im Rahmen der Novellierung des NetzDG an das Bundeskriminalamt im Fokus der Betrachtung. Im Rahmen dieser automatisierten Form der Straftatenübermittlung (die man vergleichbar aus automatisierten Meldungen über Meldestellen der Betreiber sozialer Medien im Zusammenhang mit sog. „kinderpornographischen Inhalten" kennt, dem sog. NCMEC[1] Verfahren) wurde vom Bundeskriminalamt mit etwa 250.000 Meldungen und daraus abgeleitet etwa 150.000 Ermittlungsverfahren jährlich gerechnet (Flade, 2022). Hierzu sollte angemerkt werden, dass sich die Betreiber sozialer Medien juristisch durchaus erfolgreich gegen die automatische Meldepflicht gewehrt haben, sodass entsprechende Straftaten nicht an das BKA gemeldet wurden und nun davon ausgegangen wird, dass der Digital Service Act (DSA) an Stelle des NetzDG treten könnte (Flade, 2022). Bone-Winkel diskutiert dabei in seinem Beitrag die Auswirkungen von digitaler Hasskriminalität im Allgemeinen und der Novellierung im Besonderen. Er zeigt dabei auch auf, dass gegenwärtig die Strafverfolgung im digitalen Raum bei diesem Thema an ihre Grenzen stößt und hierdurch ein Klima der ‚Enthemmung' entstehen kann. Entsprechend brauche es für eine „effektive Bekämpfung von Hass- bzw. Vorurteilskriminalität [. . .] folglich mehr als politische Absichten".

Welche Herausforderungen dann doch erlangte digitale Beweismittel – die im Rahmen von entsprechenden Straftaten anfallen können – für das deutsche Strafverfahren darstellen, beschreibt Zühlke in seinem Beitrag „Verdächtige, Verschlüsselungen und künstliche Intelligenz: Rechtsstaat 2.0". Ein besonderer Schwerpunkt bildet hierbei die Diskussion der strafprozessualen Verwertung von Informationen, die im Rahmen u. a. der „EncroChat"-Daten gewonnen bzw. von französischen Behörden übermittelt wurden. Der Autor kommt hierbei zu der Einschätzung, dass die „Datenbestände aus den EncroChat-Verfahren [. . .] in ihrer undifferenzierten Gesamtheit einem Verwendungsverbot" unterliegen würden. Dabei sieht der Autor für die Cyberkriminologie die nachvollziehbare Notwendigkeit, sich nicht nur mit klassischen Formen digitaler Kriminalität auseinanderzusetzen, sondern auch die „digitale Infrastruktur" bei regulärer Kriminalität mit in die Betrachtung aufzunehmen. Er sieht die Cyberkriminologie hierbei auch in der Pflicht, die gesellschaftliche Debatte über „Möglichkeiten und Grenzen der Strafverfolgung von Cybercrime im weiteren Sinne" voranzubringen.

Zu einer ähnlichen Erkenntnis mit einem anderen Untersuchungsfeld kommen Hoheisel-Gruler und Sowa, die das Spannungsverhältnis zwischen dem „Schutz der Privatsphäre versus polizeiliche Informationserhebungen Datenschutz und Strafverfolgung", anhand der Nutzung von Corona-Kontaktlisten durch Sicherheitsbehörden

[1] Das „National Center for Missing & Exploited Children" (NCMEC) betreibt die „CyberTipline" über die in den USA Meldungen von sog. „kinderpornographischen Inhalten" erfolgen. Dies betrifft auch die teilweise automatisierten Meldeverfahren von sozialen Medien. Im Jahr 2021 gab es nach Selbstauskunft von NCMEC 29.157.083 Meldungen in diesem Verfahren (National Center for Missing & Exploited Children, 2023). In der Folge werden diese Meldungen durch die Sicherheitsbehörden bei Hinweisen auf die Herkunft auch in andere Staaten weitergeleitet, was auch in Deutschland zu einem spürbaren Anstieg der Fallzahlen geführt hat (Bongen & Moßbrucker, 2023).

diskutieren. Das Autorenteam zeigt auf, dass mit wachsendem Datenaufkommen durch die Digitalisierung – vermutlich nachvollziehbarerweise – das Interesse der Sicherheitsbehörden an diesen Daten als Informationsquellen zur Strafverfolgung, aber auch der Gefahrenabwehr, aufkommt. Dabei sehen sie die Notwendigkeit, dass „die Sicherheit und damit die Schutzpflicht von den Grundrechten und deren Gewährleistungen her gedacht werden muss und nicht die staatlichen Befugnisse repressiver Möglichkeiten bis an die Grenze des verfassungsrechtlich Zumutbaren ausgenutzt werden".

Gerade die Legislative hat in den letzten Jahren eine Vielzahl an neuen Strafrechtsvorschriften erlassen, um damit neue digitale Entwicklungen abzudecken. Diese reichen von der Strafbarkeit des „Gefährdenden Verbreiten personenbezogener Daten" gem. § 126a StGB, was das als „Doxing" bekannte Phänomen erfasst, über die Strafbarkeit des „Betreiben krimineller Handelsplattformen im Internet" gem. § 127 StGB bis zur strafrechtlichen Erfassung der Phänomene „Upskirting" und „Downblousing" nach § 184k StGB, auch wenn Aufnahmen im digitalen Raum verbreitet werden.

Tschorr betrachtet vor dem Hintergrund der Digitalisierung die „Strafbarkeit und Rechtstaatlichkeit in Zeiten der Cyberkriminologie". Dabei erfasst Tschorr nicht nur die strafrechtliche Sichtweise, sondern diskutiert ebenfalls die verfassungsrechtlichen Herausforderungen in diesem Bereich. Dafür hat sie sich einige Rechtskonstellationen herausgesucht, an denen sie diese Herausforderungen diskutiert, etwa den Betrieb von illegalen Handelsplattformen im Darknet und die spannende Frage der Strafbarkeit von sog. „kinderpornographischen Inhalten" in einer Blockchain. Dabei kommt sie zu der generellen Schlussfolgerung, dass vor allem „legislative Schnellschüsse" den „eigentlichen Zielen" entgegenstehen, was als ein Appell an eine durchdachte und evidenzbasierte Kriminalpolitik gewertet werden kann.

Ob in einem globalen digitalen Raum ohne physisch wahrnehmbare Grenzen, also in einer digital vernetzten Welt, eine „Rechtssetzung und Rechtsdurchsetzung" überhaupt gelingen kann, wird durch Hoheisel-Gruler in seinem Beitrag zu „Das globale Dorf im Internet" kritisch betrachtet. Der Autor vergleicht dabei den digitalen Raum mit den Strukturen eines Dorfes, wo nach „Aktion und Reaktion im Endgerät der handelnden Person scheinbar räumlich zu verschmelzen scheinen", sodass Menschen das Gefühl haben, sich zwar im selben digitalen Dorf zu befinden, jedoch die NutzerInnen sich häufig in gänzlich unterschiedlichen Rechtskreisen aufhalten. Im Ergebnis kommt es also darauf an zu erkennen, dass es unterschiedliche Kriminalitätsbetrachtungen in den „jeweiligen konkreten Lebensräumen im digitalen Raum" – bildlich gesprochen den Dörfern – geben könnte. Daneben bedarf es aber im internationalen Kontext auch einer Verständigung auf gemeinsame rechtliche Strafnomen, d. h. eine Form von „Global Governance".

Während die Beiträge in Band 1 theoretische, methodische und rechtliche Ansätze der Cyberkriminologie diskutieren, nehmen sie zur gleichen Zeit unvermeidbar Bezug auf eine Vielzahl digitaler Phänomenlagen und deliktische Erscheinungsformen. Cyberkriminologische Phänomene als solche werden in Band 2 weiter beleuchtet and diskutiert, gefolgt von den organisationalen Rahmenbedingungen, die einen kompetent Umgang ermöglichen.

Band 2: „Phänomene und Auswirkungen“

Band 2 hat zum Ziel, das weite Spektrum an cyberkriminologisch relevanten Phänomenen greifbar zu machen. Auch dieser Band ist in drei Teile unterteilt. Der erste Teil sammelt Beiträge, die (cyber-)kriminologische Phänomene betrachten. Teil 2 beschäftigt sich mit Fragestellungen der Cyberviktimologie, während der abschließende Teil einen cyberkriminologischen Blick auf Organisationsperspektiven und -bedarfe nimmt.

Heil beschäftigt sich im ersten Beitrag dieses Bandes mit „Rechts-alternative Onlinestrategien und ihr[em] Gefahrenpotenzial für demokratische Gesellschaften“ und beschreibt, mit welchen Strategien rechts-alternative AkteurInnen digitale Kommunikationsmöglichkeiten einsetzen, um den Meinungsbildungsprozess zu beeinflussen. Dabei kommt sie zu dem Schluss, dass rechts-alternative AkteurInnen vor allem die teilweise „unausgereifte Gesetzeslage im Internet“ ausnutzen und die bisher „getroffenen Schutzmaßnahmen längst nicht ausreichend effektiv“ seien.

Wie notwendig eine Anpassung der digitalen Polizeiarbeit offenbar wäre, zeigt auch der Beitrag von Braasch et al., in dem die Frage der „Gewaltakzeptanz als Folge von Neutralisierungstechniken und Medienkonsum“ am Beispiel der sog. „Querdenkerbewegung“ und deren Mediennutzung diskutiert wird. Das Autorenteam kommt hierbei u. a. zu dem Ergebnis, dass neben der strafrechtlichen Komponente vor allem „der Förderung von Maßnahmen der politischen Bildung und zur Medienkompetenz oder der Schaffung von Beratungsstellen für Opfer von Hasskriminalität und digitaler Gewalt“ seitens der Politik mehr Beachtung geschenkt werden muss.

Die Gefahr, dass der digitale Raum und dessen Kommunikationsmöglichkeiten genutzt werden, um terroristische Gewalthandlungen durch Manipulationsstrategien zu initiieren, wird durch Parrino et al. in ihrem Beitrag „Wie Cyberterrorismus funktioniert und warum wir besonders wehrlos sind: Fear Engineering als primäre Taktik cyberterroristischer Akteure“ thematisiert. Der Schwerpunkt des Beitrags liegt auf der Übertragung des Konzepts des „Fear Engineering“ in den digitalen Raum bzw. der Berücksichtigung seiner Besonderheiten. Die AutorInnen grenzen den Prozess so ab, „dass sich eine cyberterroristische Taktik nur ableiten lässt, wenn Desinformationen mit dem Ziel eingesetzt werden, Angst und Schrecken zu erzeugen (Fear Engineering), um reale Gewaltausbrüche innerhalb der Gesellschaft zu provozieren oder zumindest in Kauf zu nehmen, mit der vorrangigen Absicht, die etablierte Ordnung des Systems zu zersetzen und oder zu zerstören“. Der digitale Raum zeichnet sich hierbei vor allem durch die „digitale Vernetzung, Verbreitung und Unmittelbarkeit der erlebten Wirklichkeit“ aus, während das Erleben „gleichzeitig von empirischer Realität“ abgekoppelt wird. Entsprechend sehen die AutorInnen auf der Mikroebene ihrer Analyse die Vermittlung von Medienkompetenz, die Aufklärung über grundlegende Wirkmechanismen und die Schaffung von Awareness als wichtige Gegenstrategien an.

Genauso aktuell ist der Prozess der Entwicklung extremistischer TäterInnen im digitalen Raum. Hartleb beschreibt in seinem Beitrag den „neuen Tätertypus des rechtsgesinnten ‚Lone Wolf‘ und die Unterschätzung der virtuellen Dimension“. Der

Schwerpunkt seiner Ausführungen liegt auf dem namensgebenden Konzept von rechtsgesinnten „Lone Wolfs“, die sich aber als Teil eines „größeren ideologischen Rudels“ sehen. Dabei weist er daraufhin, dass viel dafür spricht, dass „Online-Radikalisierung, also ein Radikalisierungsprozess, der vornehmlich in der virtuellen Welt stattfindet, viel effektiver ist als bisher angenommen“. Er zeigt weiterhin, dass bei mutmaßlichen EinzeltäterInnen verstärkt auch auf das im digitalen Raum geprägte ideologische Bild geachtet werden muss. Hier gäbe es gerade bei der Analyse von entsprechenden virtuellen Gemeinschaften bei den Ermittlungsbehörden Nachholbedarf. Dies zeige sich insbesondere an einer geringen Auseinandersetzung der Ermittlungsbehörden mit der Gamingcommunity – beispielhaft auf Steam (zur Thematik Polizei und Gaming vgl. auch Rüdiger, 2020b). Letztlich kommt er zu dem Schluss, dass „neue virtuell vernetzte Tätertypen entstanden [sind], die in der Gesellschaft wie in der Öffentlichkeit lediglich sporadisch als Gefahr wahrgenommen werden, bis es zur Tat kommt.“

Im gleichen Themengebiet beleuchten Staller et al. „Stochastische Gewalt und Stochastischen Terrorismus als Phänomene einer digitalisierten Welt“. Im Mittelpunkt steht die Erkenntnis, dass Kommunikation die Wahrscheinlichkeit von Gewalt und Terrorismus fördern kann, auch wenn einzelne Gewalttaten oder Akte von Terrorismus unvorherhagbar bleiben, und dass digitale Räumen für solche Kommunikation in besonderem Maße geeignet sind. Neben einer klaren Definition der Begriffe geben die Autoren Einsicht zu Wirkweisen und Prozessen sowie eine kritische Reflexion polizeilicher Kommunikation als möglicher Teil der Problematik. Der Beitrag schließt mit Lösungsvorschlägen mit Fokus auf Bildung, Counternarrativen und der Anpassung kommunikativer Haltungen.

Einen interdisziplinären Ansatz zur Betrachtung digitaler Hasskriminalität bieten Biron et al. in ihrem Beitrag zu „Hass-Postings als Form der Cyber-Kriminalität – eine interdisziplinäre Verortung“. Dabei ist der Bogen, den das Autorenteam aufspannt, breit gefächert. Neben einer eher kriminologischen Einordnung wird ein Kategorisierungsvorschlag vorgelegt, der unterschiedliche TäterInnenrollen bei der Begehung skizziert. Als eine Schlussfolgerung sieht das Autorenteam – neben Aspekte wie ein angepasster Rechtsrahmen und einer verstärkten Präventionsarbeit – interessanterweise auch die Notwendigkeit, gegen sog „Hate-Bots“ vorzugehen. Dies ist eine Forderung, die aufgrund der bereits dargelegten aktuellen Entwicklungen im Bereich der künstlichen Sprachintelligenzen, zu denen die skizzierten Medienberichte über Beleidigungen und Drohungen existieren (z. B. Herz, 2023), sicherlich nochmal an Aktualität gewinnt.

Der Beitrag „Digitale Gewalt gegen Frauen“ zeigt Hasskriminalität und digitale Gewalt, die sich gegen spezifische Gruppen richtet, in diesem Fall gegen Frauen. Meier und Ballon demonstrieren, dass dies ein grundlegendes und ungelöstes Problem im digitalen Raum ist. Neben einer ausführlichen und differenzierten Begriffsauseinandersetzung stehen vor allem die Erscheinungsformen und der Umfang mit dem Phänomen im Mittelpunkt. Dabei skizzieren die AutorInnen die Situationen, dass „weit zurückreichende Bemühungen um die Herstellung von Geschlechtergerechtigkeit keineswegs schon erfolgreich waren“, denn Frauen müssen noch stets verstärkt mit Formen digitaler Gewalt rechnen. Dementsprechend würden sich viele

Frauen weniger im digitalen Raum zeigen und äußern, was wiederum zu deren Unterrepräsentation führt.

Kudrass und Vilmar greifen in ihrem Beitrag „zur Dramaturgie der Mysogynie im Internet“ ebenfalls ausgeprägte digitale Hasskriminalität gegen Frau im digitalen Raum auf. Hierbei gehen die AutorInnen auf die unterschiedlichen Erscheinungsformen von Mysogenie ein – beispielsweise im Rahmen der sog. „Incels“ oder als Cyberharrassment – und zeigen die unterschiedlichen Viktimisierungsstufen auf. Die AutorInnen argumentieren, dass die bisherigen Handlungsmaßnahmen zur Eindämmung von digitaler Hasskriminalität durch Verlagerung der Verantwortung an die Betreiber großer sozialer Medien nicht ausreichend sind, um dieser Form von Mysogenie und digitaler Hasskriminalität zu begegnen. Dabei erachten sie die Vermittlung dieser Themen als einen wichtigen Präventionsansatz, um „Empathie- und Reflexionsvermögen“ an Schulen im Rahmen einer Medienkompetenzvermittlung zu erreichen.

Mit einem artverwandten Phänomen setzen sich Orth und Horten sich in ihrem Beitrag „Cyberstalking“ – also der digitalen Nachstellung oder Belästigung – auseinander. Bereits die erweitere Überschrift „neue Erscheinungsformen eines alten Phänomens“ zeigt auf, dass die Autorinnen Cyberstalking nicht unbedingt als ein gänzlich neues, digitales Phänomen betrachten, sondern als eine neue Erscheinungsform der bereits bekannten Nachstellung einstufen. Als Besonderheiten arbeiten sie heraus, dass es CyberstalkerInnen im digitalen Raum sehr einfach fällt, Opfer zu schaden, und sich TäterInnen gleichzeitig durch die gemutmaßten Formen von Anonymität sicher fühlen können. Dabei wird auch herausgearbeitet, dass mehrheitlich Frauen von Formen des Cyberstalking betroffen sind.

Eine weitere Ausprägung von Delikten, die sich auf spezifische Gruppen richten, sind Straftaten gegen Kinder und Jugendliche. Kinder sind auch im digitalen Raum oft ungefiltert allen digitalen Risiken, von Hasskriminalität bis zu Sexualdelikten, ausgesetzt, mit denen auch Erwachsene konfrontiert werden. Sexualdelikte wie beispielsweise Cybergrooming – also dem „onlinebasierten Einwirken auf ein Kind mit dem Ziel der Einleitung oder Intensivierung eines sexuellen Kindesmissbrauchs“ – werden durch Minderjährige stellenweise als eine Art Normalität des digitalen Raums wahrgenommen (Rüdiger, 2020a). Dies liegt sicherlich auch daran, dass es der digitale Raum gerade SexualtäterInnen besonders leicht macht, Delikte zu begehen.

Steffes-enn und Ihm beschreiben in ihrem Beitrag zu „Pädosexuellen Überzeugungstätern im Netz“, wie der digitale Raum es pädokriminellen TäterInnen ermöglicht, sich weltweit zu vernetzen. Dabei bewegen sich die TäterInnen teilweise auf entsprechend abgekapselten digitalen Plattformen, auf denen diese weitestgehend unter sich sind. Dadurch würden die „devianten Fantasien ungebremst kommuniziert und wechselseitig bestärkt“. Die Autorinnen kommen zu der Schlussfolgerung, dass auch in den nächsten Jahren mit einem weiteren Anstieg dieses Phänomens zu rechnen ist. Der Cyberkriminologie käme hierbei die Funktion zu, durch eine weitere Differenzierung der Phänomenlage bessere Möglichkeiten der Rückfallprävention und Ermittlungsarbeit zu entwickeln.

Manipulationen, Initiierungen und Groomingmechanismen im digitalen Raum finden dabei nicht nur bei SexualtäterInnen und im Bereich Terrorismus statt. Dass auch Gruppen der organisierten Kriminalität Formen der Selbstdarstellungen in den Sozialen Medien nutzen und einer Form des digitalen Narzissmus fröhnen, um ihren „Lifestyle" zu präsentieren, „Rivalen herauszufordern" oder damit Nachwuchswerbung zu betreiben, zeigen Peteranderl und Jaroschewski in ihrem Beitrag zur „Organisierten Kriminalität auf TikTok". Hierzu haben die beiden Autorinnen Profile auf TikTok von unterschiedlichen kriminellen Organisationen aus dem amerikanischen (u. a. Honduras, Mexiko, Brasilien und die USA) sowie europäischen Raum (u. a. Großbritannien und Italien) untersucht. Dabei kommen sie zu dem Schluss, dass TikTok weniger „als strategischer PR-Kanal krimineller Gruppierungen genutzt" wird, „sondern vor allem als Plattform, auf der Mitglieder krimineller Organisationen privat posten". Diese Darstellungen können aber zur „Glorifizierung krimineller Organisationen" beitragen, wenn bspw. teure Luxusgegenstände gepostet werden. Dabei sehen die Autorinnen den Trend, dass TikTok ebenso wie Ermittlungsbehörden vermehrt gegen diese Entwicklung vorgehen, die kriminellen Gruppierungen jedoch Wege finden Filtermechanismen zu umgehen.

Längst haben sich auch Formen organisierter Kriminalität entwickelt, die sich weitestgehend auf digitale Kriminalitätsformen spezialisiert haben. Eine, auch bei der medialen Berichterstattung besonders im Fokus liegende Aktivität, sind Angriffe durch sog. „Ransomware", also Erpressungssoftware. Atug greift das Thema von „Ransomware als Business Case in der organisierten Kriminalität" auf und stellt hierbei vor allem die Angreifergruppen in den Mittelpunkt seiner Analyse. Neben der Darstellung des Modi Operandi zur „Verschlüsselung kritischer Unternehmensdaten" zeigt der Autor, dass es einigen Gruppen durchaus um einen „Ruf der Professionalität" oder sogar des „Humanismus" gehen würde und beispielsweise „Regeln gegen Angriffe auf Krankenhäuser und gemeinnützige Organisationen" aufgestellt hätten, auch vor dem Hintergrund der Corona-Pandemie. Dennoch gab es Angriffe auf Krankenhäuser, weil dies einen „hochprofessionalisierten und sehr lukrativen Schattenmarkt" darstellt. Dass auch Sicherheitsbehörden Grenzen gesetzt sind, wird dadurch deutlich, dass selbst Polizeibehörden – z. B. in Großbritannien – Ransomware-Angriffen ausgesetzt sind. Entsprechend sieht der Autor vor allem die Firmen, Institutionen und Behörden in der Pflicht, sich durch Schutzmaßnahmen zu wappnen, denn mit einer Entspannung der Situation sei nicht zu rechnen.

Gerade in den ersten Wochen des russischen Angriffskrieges gegen die Ukraine im Jahr 2022 haben in Deutschland sicherlich viele – vor allem auch jüngere – Menschen Schreckensnachrichten und Videos von Kriegssituationen in den Sozialen Medien konsumiert. Ein Problem ist, dass die Algorithmen dazu tendieren, kontinuierlich ähnliche Inhalte zu zeigen; ein Phänomen, dass schnell zu dem sog. „Doomscrolling" führen kann, das man also nur noch „Schreckensnachrichten" konsumiert. Dass Soziale Medien auch für die Kriegsführung eine immer stärkere Rolle spielen, wird von Bergmann und Petrossian ihrem Beitrag „Psychologische und digitale Kriegsführung durch die informelle Verbreitung von Kriegsverbrechen" gezeigt. Dabei stützen sich die Autoren auf „empirische Befunde des dritten Krieges um Berg-Karabach im Herbst 2020" und zeigen, dass Kriege und bewaffnete Kon-

flikte immer stärker auch im digitalen Raum – vor allem in Form des sog. Informationkrieges – stattfinden. Dabei nehmen „informelle Publikationswege in sozialen Medien eine immer wichtigere Position in diesem digitalen Phänomen" ein. Die Autoren entwickeln eine Übersicht zu Ausprägungen psychologischer Kriegsführung und deren sozialpsychologischen Auswirkungen und plädieren für die Notwendigkeit, dass „in Zukunft effizientere Maßnahmen der Plattformbetreiber zum Schutz der User ergriffen" werden müssen. Dies ist eine Forderung, die vor dem Hintergrund der vielen minderjährigen NutzerInnen, die dadurch Formen der Viktimisierung erleiden können, sicher eine besondere Bedeutung hat.

Neue Delikte und Phänomene entstehen, wo eine Verschmelzung zwischen Technik, Biologie und dem Menschen denkbar wird. Waren technische Implantate zur Verschmelzung von Mensch und Technik früher eher SciFi-Genres wie dem „Cyberpunk" vorbehalten, ist diese Entwicklung heute greifbar. So verkündete die Elon Musk Firma Neuralink in 2022, einen Computerchip für das Gehirn als digitale Schnittstelle entwickeln zu wollen. Auch wenn Experimente am Menschen bisher durch die zuständigen amerikanischen Behörden verwehrt wurden, wirft dieses Feld doch große Fragen für die Cyberkriminologie auf (Levy & Tylor, 2023). Denn was passiert z. B. wenn ein solcher Chip digital angegriffen wird? Butz und Höffler greifen mit ihrem Beitrag „Cyberbiokriminalität und Cyberbiosicherheit – Kriminologische Überlegungen im Angesicht von biotechnologischen Entwicklungen" dieses neuartige Forschungsfeld auf. Dabei stellen sie zunächst Begriffsentwicklungen und Hintergründe vor, um dann Überlegungen zu Ursachen und praktische Präventionsansätze zu entwickeln. Die möglichen Kriminalitätsformen, die sich aus aktuellen Entwicklungen der Biotechnologie ergeben, sind dabei äußerst vielfältig. Angefangen mit Bio-Diskriminierung durch Ausnutzung unrechtmäßig erworbener DNA-Daten über die Manipulation von DNA-Sequenzen, die die Produktion schädlicher Organismen oder das Hacken von Software erlaubt (Bio-Malware) bis hin zu „biotechnologisch fundierter Betäubungs- und Arzneimittelkriminalität" und Bio/Neuro-Hacking ist vieles denkbar und möglich und weitere Möglichkeiten werden in dem Kapitel systematisch beschrieben. Die AutorInnen diskutieren weiterhin die Übertragbarkeit theoretischer Ansätze als Erklärungsansaetze für Kriminalität und Täter in diesem neuen Bereich. Angesichts der kriminogenen Relevanz von Biotechnologien halten es die AutorInnen für entscheidend, dass die Kriminologie sich verstärkt an „den gesellschaftlichen Bewältigungs- und Aushandlungsprozessen" solcher Innovationen beteiligt sowie Erklärungs- und Präventionskonzepte entwickelt, die sowohl technische als auch soziale Aspekte einbeziehen.

Die Frage, welche Auswirkungen die Konfrontation mit digitalen Delikten auf die NutzerInnen oder auch Institutionen haben können, steht im Mittelpunkt der Beiträge des zweiten Teils von Band 2. Weber und Wührl kommen in ihrem Beitrag „Opfererfahrungen im Internet – Ergebnisse des Deutschen Viktimisierungssurvey (DVS)" zu der Schlussfolgerung, dass die Anzeigequoten bei Cyberdelikten eher niedrig sind. Dabei zeigen die Autorinnen auf, dass „die Anzeigebereitschaft mit der wahrgenommenen Schwere des Opfererlebnisses zusammenhängt, aber nicht mit dem berichteten Vertrauen in die Polizei". Sie geben zudem zu bedenken, dass „bei Cyber-Delikten auch das doppelte Dunkelfeld eine Rolle spielt, welches durch Dunkelfeldbefragungen nicht aufgehellt werden kann, da sich die Betroffenen zum

Teil selbst nicht darüber im Klaren sind, dass sie Opfer einer Straftat wurden“. Sie kommen weiterhin zu der Erkenntnis, dass „im Internet nahezu jeder gleichermaßen dem Risiko ausgesetzt ist, Opfer einer Cyber-Straftat zu werden“, also die Frage, ob man eine Viktimisierung im digitalen Raum erlebt „nicht an das soziodemografische Profil einer Person gebunden“ zu sein scheint.

Müller et al. setzen den Schwerpunk in ihrem Beitrag „Viktimisierungen durch Cybercrime: Psychische Folgen und Reaktionen“ auf individuelle Auswirkungen. Kernstück des Beitrags ist die Präsentation von Ergebnissen eines Forschungsprojekt des Kriminologischen Forschungsinstituts Niedersachsen (KFN) zur Erhellung des Dunkelfelds bei der Konfrontation mit digitalen Delikten. Im Rahmen des Projekts wurden etwa 4000 Menschen ab 16 Jahren in Niedersachsen zu deren Opfererfahrungen bei digitalen Delikten befragt. Zudem wurden mit konkret betroffenen Personen 20 qualitative Interviews durchgeführt. Im Ergebnis gaben etwa 38 % der Befragten an, „in ihrem Leben mindestens einmal durch irgendeine Form von Cybercrime im weiteren Sinne viktimisiert“ worden zu sein. Dabei gaben die Befragten an, in den letzten 12 Monaten vor der Befragung am häufigsten von Cyberstalking (11 %), sexueller Belästigung (9 %) und Formen von Online Waren-/Kreditbetrug (8 %) betroffen gewesen zu sein. Nur ein geringer Teil von 14 % brachte die erlittenen Viktimisierungen auch zur Anzeige, wobei als häufigste Motivation der Wunsch angegeben wurde, dass TäterInnen bestraft werden sollten. Die AutorInnen zeigen auf, dass „Viktimisierungserfahrungen in Bezug auf Cybercrime ernstzunehmende Folgen nach sich ziehen können“.

Mit dem Reaktionsverhalten von Betroffenen setzen sich auch Stevens et al. in ihrem Beitrag „Wie gehen Verbraucher:innen mit Onlinebetrug um?“ auseinander. Es handelt sich bei dem Beitrag um eine Literaturübersicht fokussiert auf Verbraucher, die u. a. eine Kategorisierung der unterschiedlichen Erscheinungsformen von Betrugshandlungen im digitalen Kontext vornimmt. Neben den Modi Operandi wird die Studien- und Literaturlage zu Opferprofilen und Tatauswirkungen analysiert. Des Weiteren wird auf „Hilfeangebote und Anlaufstellen für Betroffene“ eingegangen. Im Ergebnis werden vor allem die noch sehr geringen „praktischen Hilfsangebote von offizieller Seite“ kritisch bewertet. Interessanterweise betont das Autorenteam auch die verstärkte Verantwortung der Unternehmen, wenn auf ihren Plattformen NutzerInnen eine Viktimisierung erfahren. Hier sehen sie zahlreiche Verbesserungsmöglichkeiten.

Mit „Hilfeeinrichtungen für Opfer von Cyberkriminalität“ als potenzielle Anlaufstellen für Betroffene hat sich Drafz in ihrem Beitrag mit Fokus auf drei Opferberatungsstellen in Deutschland und deren Umgang mit Cyberkriminalität auseinandergesetzt. Neben einer generellen Einführung in das System der Opferhilfe in Deutschland, stellt die Autorin fest, dass sich die Opferhilfe in Deutschland generell erst seit jüngerer Zeit ernsthaft auf digitale Kriminalitätsformen einstellt und sich weiterhin „die viktimologische Forschung in diesem Bereich noch relativ am Anfang befindet“. Daher sei „die Frage noch ungeklärt, ob Opfer von Cyberkriminalität überhaupt Unterstützung bei der Bewältigung des Tatgeschehens benötigen und falls ja, wie diese am besten gestaltet werden kann“. Eventuell ist diese Unsicherheit auch einer der Gründe, warum der Autorin zu Folge die Beratungsstellen „vor allem auf Informationsmaterial für PrivatnutzerInnen im Internet setzen“. Als einen Lösungs-

ansatz schlägt die Autorin u. a. eine „Fusion [von] Anlaufstellen zu einer einzigen Opferberatungseinrichtung und eine Vereinigung der angesprochenen Inhalte zu einem Ansatz“ vor.

Dass auch „Unternehmen als Opfer von Cyberkriminalität“ in Erscheinung treten, thematisieren Dreißigacker et al. in ihrem gleichnamigen Kapitel. Im Mittelpunkt der Ausführungen steht die Auswertung einer groß angelegten, zweiphasigen Befragung von 5.000 Unternehmen zu den Erscheinungsformen von Cyberkriminalität und deren Auswirkungen. Dabei zeigte sich, dass in der ersten Befragungsphase 41,1 % und in der zweiten Phase 59,6 % der Unternehmen von mindestens einem digitalen Angriff in den letzten 12 Monaten berichten konnten. Als häufigste Angriffsformen wurden hierbei die Konfrontation mit Phishing und sonstige Malware- und Ransomware-Angriffe genannt. Der durchschnittliche Vermögensschaden bewegte sich gemäß Umfrage zwischen 16.900 Euro in der ersten Erhebungsphase und 7.780 Euro in der zweiten Phase. Dabei kommt auf die Ermittlungsbehörde noch einiges zu. Denn bisher haben „die Strafverfolgungsbehörden im Verhältnis zum Tataufkommen wenig Zugang zu diesem Bereich [. . .] und werden, ausgedrückt in einer geringen Anzeigebereitschaft, häufig noch nicht einmal als Ansprechpartner wahrgenommen“.

Meywirth, Pauker und Sowa diskutieren in ihrem Beitrag „Cybercrime und Cyber Security Intelligence – kollaborative Ansätze gegen Cyber- und Computerkriminalität“ anhand aktueller digitaler Bedrohungslagen unter anderem auch das Verhältnis zwischen Sicherheitsbehörden und Unternehmen. Hierbei werden von den AutorInnen unterschiedliche Ansätze der Kooperation zwischen den AkteurInnen zur präventiven Begegnung, etwaigen Reaktionen aber auch zur Detektion von Cybercrime Delikten vorgestellt und eingeordnet. Dabei ordnen sie vor allem Cybercrime im engeren Sinne als ein strategisches Thema für Politik und Wirtschaft ein, das in Relevanz in Zukunft vermutlich nur noch zunehmen wird.

Der dritte und letzte Teil des zweiten Bandes beschäftigt sich mit Organisationsperspektiven im Kontext der Cyberkriminologie. Den Auftakt macht ein Beitrag von Baumgartner zur „Digitalen Polizeiarbeit der Zukunft“, der vornehmlich aus der Perspektive der österreichischen Sicherheitsbehörden verfasst ist. Entsprechend betont Baumgartner bereits zu Beginn, dass der Beitrag auch auf seinen 30 Jahren Erfahrungen in der österreichischen Polizei beruht, weist aber darauf hin, dass zwar die digitale Polizeiarbeit von Land zu Land unterschiedlich sein kann, aber die Problemstellungen ähnliche sind. So müssten sich beispielsweise alle Polizeien mit der immensen Flut an Daten auseinandersetzen, was auch unter dem Phänomen „Big Data“ bekannt ist. Neben der Beschreibung klassischer digitaler Problemstellungen wie der Ermittlung von IP-Adressen, die mutmaßliche Anonymität oder der Einsatz von forensischer Software beschreibt Baumgartner auch die individuellen Herausforderungen von Polizeibehörden. Dazu gehört die Frage, welche Fachkenntnisse ErmittlerInnen benötigen, oder auch wie polizeilicher Nachwuchs für diesen Bereich gewonnen werden kann. Besonders den Aspekt „Human Ressources im Bereich der digitalen Polizeiarbeit“ zu sichern, hält er für einen wichtigen Eckpfeiler einer zukunftsorientierten Polizeiarbeit.

Staller und Koerner beschreiben, wie digitale Themen im Rahmen des polizeilichen Einsatztraining behandelt werden können und sollten. In ihrem Beitrag „Einsatztraining und Digitalität" analysieren die Autoren das Thema auf drei Ebenen: Einsatztraining für die digitale, mit der digitalen und in der digitalen Welt. Das Einsatztraining für die digitale Welt bietet u. a. eine systematische Übersicht über die unterschiedlichen Studien- und Fortbildungsmöglichkeiten für PolizistInnen und zeigt den vorhandenen Anpassungsdruck der Sicherheitsbehörden bei digitalen Themen auf. Training mit der digitalen Welt wird durch die Autoren einerseits so definiert, dass die Polizei durch digitalisierte Mustererkennungen Erkenntnisse gewinnen kann, die z. B. konkrete inhaltliche Schwerpunkte vorgeben könnten. Die Debatte, die die Autoren hier aufwerfen, könnte sicherlich zukünftig an Fahrt gewinnen, wenn beispielhaft Künstliche Intelligenz beginnt, Trainings zu gestalten und auszuwerten. Die Nutzung von Virtual Reality platziert polizeiliches Training in die digitale Welt. Hier stellen die Autoren zunächst die Frage, warum trotz aller Vorhersagen Virtual Reality im polizeilichen Training bisher kaum eine Rolle spielt. Die Autoren vermuten, dass durch technologische Entwicklungen (man denke an leistungsfähige Grafik, verbesserte Immersion, z. B. mit Force Feedback Technologien usw.) Virtual Reality immer „modern und innovativ erscheinen" kann und dass diese für Forschungsprojekte deshalb häufig attraktiv erscheinen. Sie warnen jedoch auch, dass Virtual Reality zwar Potenziale habe, aber nicht das „Kernproblem trainingspädagogischer Gestaltung löst". Ihr Fazit ist daher auch eher ernüchternd, denn die Digitalisierung kann grundsätzliche Problemstellungen beim Einsatztraining nicht auflösen.

Dies ist ein Thema, das Honekamp et al. mit ihrem Beitrag zu „Technologiegetriebener Polizeiausbildung im Umgang mit Digitalen Spuren" mit einer etwas anderen Ausrichtung ebenfalls aufgreifen. Dabei steht die Frage im Mittelpunkt, welche „Anforderungen [sich] an die Ausbildung im polizeilichen Umgang mit digitalen Spuren" stellen. Die Autoren erörtern im Rahmen ihres Beitrags, ob digitale Spuren „an der Schwelle" stehen würden, „Teile der klassischen Kriminalität und Spurenlagen zu ersetzen" oder diese Schwelle bereits überschritten wurde. Dabei liegt der Fokus explizit auf Anforderungen im Rahmen des sog. „ersten Angriffs", also Erstmaßnahmen bei der Anzeigenaufnahme. Als Datengrundlage wurden u. a. die Modul- und Studienhandbücher aller 16 Bundesländer herangezogen. Die Autoren kommen hierbei zu dem Ergebnis, „dass die derzeitige Ausbildung im Bezug auf Digitale Spuren in den meisten Bundesländern angepasst werden müsste". Entsprechend kommen sie zu dem generellen Fazit, dass die PolizeianwärterInnen aller Länder „durch eine adäquate und zukunftsgerichtete Ausbildung auf ihre tägliche Polizeiarbeit in der immer mehr digitalisierten Welt bestmöglich vorbereitet werden" müssen.

Das abschließende Kapitel des Bandes wird von Piasecki mit einem Beitrag zu „Computer- und technologievermittelte Kommunikation als sozialer Faktor im Dienstverhältnis" beigesteuert. Im Kern beschäftigt sich dieser Beitrag mit der missbräuchlichen Nutzung vor allem von Sozialen Medien und Messengern durch PolizeibeamtInnen; ein Umstand, der in den letzten Jahren vor allem im Zusammenhang mit menschenverachtenden Beiträgen in Chatgruppen diskutiert wurde. Piase-

cki diskutiert im Rahmen seines Beitrages daher einerseits gruppendynamische Prozesse bei der Nutzung Sozialer Medien. Andererseits setzt er sich mit der Nutzung von „Social Media Technologien" (SMT) im polizeilichen Alltag auseinander. Diese würde zwar eine schnelle Kommunikation im dienstlichen Alltag ermöglichen, andererseits würden sie aber auch zu persönlichen Kommunikationen verleiten. Am Beispiel der Polizei NRW beschreibt der Autor, dass SMT im polizeilichen Alltag zwar verankert sind, hier aber eigene polizeiliche Social-Media-Apps einschließlich eines Messengers für dienstliche Smartphones entwickelt wurden. Piasecki sieht vor allem die Notwendigkeit der Vermittlung von „Grundkompetenzen in der Medienanwendung".

Epilog

Während wir sehr froh sind über die Diversität an Expertise, die unser Handbuch repräsentiert und ermöglicht, sind wir uns auch bewusst, dass zwei Bände keinesfalls ausreichen, um die komplette theoretische, methodische, phänomenologische und praktische Bandbreite der Cyberkriminologie auszuleuchten. Dieses Vorhaben wäre vergleichbar mit einem Handbuch, dass alle Aspekte von sozial abweichenden Verhaltensweisen und der Arbeit der Kontrollmechanismen im physischen Raum, abbilden würde. Unser Anliegen mit diesem Handbuch ist es daher, eine Basis zu schaffen, von der aus weitere Erkundungen möglich werden und diese (hoffentlich) auch animiert.

Dies ist notwendig, denn die Cyberkriminologie ist ein Feld, dass kontinuierlich in Bewegung sein muss. Innovationen wie Künstliche Intelligenz – mit Anwendungen wie ChatGTP und Deep Fakes – das Metaverse oder auch die Nutzung von autonomen Robotern, die heute neu und verstörend erscheinen, werden in ein paar Jahren vermutlich ein (fast) normaler Bestandteil unserer Lebenswirklichkeit sein. Das lässt sich wunderbar am Beispiel der polizeilichen Nutzung sozialer Medien beobachten, die wir selbst über die letzten zwölf Jahre intensiv mitverfolgt haben (z. B. Denef et al., 2011; Akhgar et al., 2019; Bayerl & Rüdiger, 2017, 2022; Rüdiger, 2019; Rüdiger & Denef, 2013). Was 2010 noch als ‚blosser Jugendtrend', flüchtige Erscheinung und vermutlich irrelevant für die Polizeiarbeit diskutiert wurde, ist heute ein gebräuchlicher (wenn auch nicht in allen Formen akzeptierter) Teil polizeilichen Arbeitens. Wir sehen eine der Rollen der Cyberkriminologie darin, traditionelle Ansätze zu überprüfen, zu hinterfragen und auf neue Entwicklungen anzupassen, und noch wichtiger, Kreativität und theoretische, methodische sowie praktische Innovationen zu fördern.

Die Bedeutung von online und digitalen Welten, von Vernetzung und Automatisierung wird in allen Lebensbereichen ohne Zweifel weiter steigen. Und ebenso sind neue Trends und Innovationen unvermeidbar. Das Verstehen und die kritische Reflektion darüber, was dies heisst für Opfer, TäterInnen und Gesellschaft, für individuelle und kollektive Sicherheit im nationalen und internationalen Rahmen sowie für die Organisationen, die mit Verbrechensbekämpfung und -prävention betraut sind, muss deshalb kontinuierlich, systematisch und energisch geführt werden.

Wir verstehen unser Handbuch deshalb sowohl als ein Kompendium, dass den derzeitigen Stand an Wissen und Diskussionen in der Cyberkriminologie skizziert, als auch als eine Einladung an AkademikerInnen und PraktikerInnen dieses wichtige Feld gemeinsam weiter zu entwickeln.

Thomas-Gabriel Rüdiger
Petra Saskia Bayerl

Literatur

Akhgar, B., Bayerl, P. S., & Leventakis, G. (2019). *Social media strategy in policing. From cultural intelligence to community policing* (Security informatics and law enforcement Ser). Springer International Publishing AG.

Bayerl, P. S., & Rüdiger, T.-G. (2017). Die polizeiliche Nutzung sozialer Medien in Deutschland: Die Polizei im digitalen Neuland. In J. Stierle, D. Wehe, & H. Siller (Hrsg.), *Handbuch Polizeimanagement. Polizeipolitik – Polizeiwissenschaft – Polizeipraxis* (S. 919–943). Springer Gabler.

Bayerl, P. S., & Rüdiger, T.-G. (2022). Die polizeiliche Nutzung Sozialer Medien in Deutschland: Zwischen Kommunikation, Globalität und Digitaler Kriminalitätstransparenz. In D. Wehe & H. Siller (Hrsg.), *Handbuch Polizeimanagement* (S. 1–29). Springer Fachmedien Wiesbaden.

Beuth, P. (2016). Microsoft: Twitter-Nutzer machen Chatbot zur Rassistin. In *Die Zeit*, 24.03.2016. Zugegriffen am 18.06.2022.

Bongen, R., & Moßbrucker, D. (2023). Sexualisierte Gewalt gegen Kinder: Gesetzesverschärfung soll korrigiert werden. In *tagesschau.de*, 10.03.2023. Zugegriffen am 16.03.2023.

Denef, S., Bayerl, S. P., & Kaptein, N. (2011). Cross-European approaches to social media as a tool for police communication. *CEPOL European Police Science and Research Bulletin, 6*, 11–14.

Deutscher Bundestag. (2023). Deutscher Bundestag – Forschungsausschuss gibt Studie zu Auswirkungen von ChatGPT auf. https://www.bundestag.de/presse/pressemitteilungen/2023/934052-934052. zuletzt aktualisiert am 07.03.2023, Zugegriffen am 07.03.2023.

Flade, F. (2022). Hasskriminalität im Netz: BKA wartet auf Meldungen. In *tagesschau.de*, 31.05.2022. https://www.tagesschau.de/investigativ/wdr/bka-zentralstelle-hasskriminalitaet-internet-101.html. Zugegriffen am 08.03.2023.

Handelsblatt. (2023). Microsoft schränkt Nutzung von Bing-Chatbot nach verwirrenden Antworten ein. In *Handelsblatt*, 19.02.2023. https://app.handelsblatt.com/technik/it-internet/kuenstliche-intelligenz-microsoft-schraenkt-nutzung-von-bing-chatbot-nach-verwirrenden-antworten-ein/28990946.html. Zugegriffen am 16.03.2023.

Herz, F. (2023). Chat-KI erklärt Münchner Studenten zum Feind – weil er zu viele Fragen stellt. https://www.merkur.de/lokales/muenchen/muenchen-chat-ki-bing-gpt-microsoft-kuenstliche-intelligenz-fragen-ztz-92109417.html. zuletzt aktualisiert am 08.03.2023, Zugegriffen am 08.03.2023.

HpolBB. (2021). Institut für Cyberkriminologie an der Hochschule gegründet. Hochschule der Polizei des Landes Brandenburg (HpolBB). https://hpolbb.de/article/institut-f%C3%BCr-cyberkriminologie-der-hochschule-gegr%C3%BCndet.

Krischok, H. (2018). Das Internet in der polizeilichen Gefahrenabwehr. In T.-G. Rüdiger & P. S. Bayerl (Hrsg.), *Digitale Polizeiarbeit. Herausforderungen und Chancen* (Research, S. 237–257). Springer VS.

Levy, R., & Tylor, M. (2023). U.S. regulators rejected Elon Musk's bid to test brain chips in humans, 02.03.2023. https://www.reuters.com/investigates/special-report/neuralink-musk-fda/. Zugegriffen am 09.03.2023.

MDR. (2022). Deepfake: Manipulierte, aber echt wirkende Medieninhalte. In *MDR*, 13.05.2022. https://www.mdr.de/nachrichten/deutschland/panorama/manipulation-stimme-deepfake-technologie-100.html. Zugegriffen am 07.03.2023.

Meister, A. (2022). Strafrecht: Die meisten Tatverdächtigen bei „Kinderpornografie" sind minderjährig. https://netzpolitik.org/2022/strafrecht-die-meisten-tatverdaechtigen-bei-kinderpornografie-sind-minderjaehrig/. zuletzt aktualisiert am 16.03.2023, Zugegriffen am 16.03.2023.

Meta. (2021). Connect 2021: Our vision for the metaverse, zuletzt aktualisiert am 28.10.2021, Zugegriffen am 07.03.2023.

National Center for Missing & Exploited Children. (2023). CyberTipline Data. https://www.missingkids.org/gethelpnow/cybertipline/cybertiplinedata. zuletzt aktualisiert am 24.02.2023, Zugegriffen am 16.03.2023.

Rüdiger, T.-G. (2019). Polizei im digitalen Raum. *Zeitschrift der Bundeszentrale für Politische Bildung (APUZ), 69*(23-23/2019), 18–23.

Rüdiger, T.-G. (2020a). *Die onlinebasierte Anbahnung des sexuellen Missbrauchs eines Kindes*. Dissertation. Universität Potsdam.

Rüdiger, Thomas-Gabriel (2020b): Polizei und Gaming – The next Level? Games und die Polizei – Das missverstandene Medium. In *Polizei Verkehr und Technik (PVT), 06*(2020), S. 26–29.

Rüdiger, T.-G. (2021). Digitale Kriminalitätstransparenz – Von der Durchbrechung der Präventivwirkung des Nichtwissens. *Kriminalistik, 2021*(2/2021), 72–78.

Rüdiger, T.-G. (2023). Cyberkriminologie – Von digitaler Kriminalitätstransparenz bis zum Broken Web. In D. Wehe & H. Siller (Hrsg.), *Handbuch Polizeimanagement. Polizeipolitik – Polizeiwissenschaft – Polizeipraxis* (2. Aufl., S. 941–964). Springer Gabler.

Rüdiger, T.-G., & Bayerl, P. S. (2020). Cyberkriminologie. In T.-G. Rüdiger & P. S. Bayerl (Hrsg.), *Cyberkriminologie* (S. 3–12). Springer Fachmedien Wiesbaden.

Rüdiger, T.-G., & Denef, S. (2013). Soziale Medien – Muss sich die Polizei neu ausrichten. *Deutsche Polizei*, (11), 4–14. www.gdp.de/gdp/gdp.nsf/id/dp201311/$file/DP_2013_11.pdf

Takagi, Y., & Nishimoto, S. (2023). Stable diffusion with brain activity. School of Frontier Biosciences, Osaka University. https://sites.google.com/view/stablediffusion-with-brain/home?authuser=0. zuletzt aktualisiert am 16.03.2023, Zugegriffen am 16.03.2023.

Wiley, J. (2007). *Second Life. Das offizielle Handbuch* (1. Aufl.). Wiley-VCH.