ROAR Handbuch

Vom Verstehen und Verhindern von Cyberkriminalität bis hin zur Unterstützung und Stärkung von Cyberkriminalitätsopfern

ROAR
empowering
victims of
cybercrime

APAV
associação portuguesa de
Apoio à Vítima

Diese Veröffentlichung wurde durch den Fonds für die innere Sicherheit der Europäischen Union — Polizei finanziert

Durchgeführt von:
Associação Portuguesa de Apoio à Vítima (APAV) | Portugal

Projektpartner:
Ministério da Administração Interna (MAI) | Portugal
Procuradoria-Geral da República (PGR) | Portugal
PT Portugal | Portugal
Weisser Ring e.V. | Deutschland
ACTEDO | Rumänien

ISBN: 978-989-54855-8-1
Legal Deposit:

Titel:
ROAR Handbuch – Vom Verstehen und Verhindern von Cyberkriminalität bis hin zur Unterstützung und Stärkung von Cyberkriminalitätsopfern

Adresse:
APAV – Associação Portuguesa de Apoio à Vítima
Rua José Estêvão, 135 A
1150-201 Lissabon - Portugal

Tel.: +351 213 587 900
E-mail: apav.sede@apav.pt
Webseite: www.apav.pt
Facebook: www.facebook.com/APAV.Portugal

INHALTSVERZEICHNIS

INHALTSVERZEICHNIS

TEIL I
VERSTEHEN

TEIL I

VERSTEHEN

1. CYBERKRIMINALITÄT: EINE KONZEPTUALISIERUNG

1.1. Informations- und Kommunikationstechnologien (IKT) und die Entstehung der Cyberkriminalität

HIGHLIGHT | DATEN IM FOKUS:

Laut EUROSTAT[1] hatten im Jahr 2017 87 % der Haushalte in der Europäischen Union einen Internetzugang. Im Vergleich dazu waren es 2010 noch 70 % gewesen.

Mehr als 85 % der Befragten gaben an, das Internet täglich zu nutzen. Die höchsten Nutzungsanteile wurden in Italien, Dänemark, Malta, den Niederlanden und Schweden festgestellt.

EUROSTAT untersuchte außerdem die Nutzung des Internets durch Unternehmen und Organisationen: lediglich 3 % der Unternehmen in der Europäischen Union hatten 2017 kein Internet. Der höchste Anteil der Unternehmen ohne Internet wurde in Rumänien und Griechenland festgestellt.

In der gleichen Umfrage erfasste EUROSTAT einige E-Commerce-Indikatoren[2]: Während der letzten 10 Jahre stieg die Häufigkeit des Onlineshoppings in allen Altersgruppen der Internetnutzer, ganz besonders bei Jugendlichen und jungen Erwachsenen im Alter von 16 bis 24 Jahren. Die Umfrage unter Organisationen und Unternehmen ergab außerdem, dass 2017 20 % der Unternehmen E-Commerce betrieben.

Die o. g. Daten (und andere Informationsquellen) zeigen die zunehmende Nutzung des Internets in verschiedenen Bereichen, besonders in der Europäischen Union. Sie stützen die These, dass das Internet tatsächlich und zunehmend global, unmittelbar und grenzübergreifend ist und eine dezentrale Netzwerkstruktur für die digitale Verbreitung von Informationen bereitstellt (Koops, 2010).

Das Internet und Informations- und Kommunikationstechnologien (IKT)[3] haben aufgrund dieser Merkmale die Begehung von Straftaten sowohl vereinfacht als auch neue Möglichkeiten geschaffen, indem sie diese Möglichkeiten verändert und vervielfacht haben, entweder, weil sie selbst potenzielle Ziele krimineller Handlungen sind oder weil sie die Mittel und Werkzeuge für die Begehung anderer krimineller Handlungen darstellen (Van Wilsem, 2011).

Das Internet hat **neue Formen und Möglichkeiten zur Verübung „herkömmlicher" Straftaten geschaffen**, wie Stalking, sexueller Missbrauch von Kindern oder Betrug, aber es hat auch die **Entstehung neuer Formen von Kriminalität** ermöglicht, die ausschließlich mithilfe von Computern, IKT und Computersystemen begangen werden können, wie Hackerangriffe, DDoS und Schadsoftware, die in den folgenden Kapiteln dieses Handbuchs erläutert werden. (Yucedal, 2010; Jahankhani, Al-Nemrat & Hosseinian-Far, 2014).

Bei näherer Betrachtung haben die durch das Internet bereitgestellten Ressourcen, die „transformativen Elemente", **die Art und Weise revolutioniert, wie Verbrechen begangen werden können** (Wall, 2007 *cit in* Jahankhani et al., 2014). Wir beziehen uns auf die folgenden Aspekte, die durch das Internet entweder begünstigt oder erst ermöglicht wurden:

[1] *Digital economy & society in the EU - A browse through our online world in figures | 2018 edition*, abrufbar unter https://ec.europa.eu/eurostat/cache/infographs/ict/index.html.

[2] Das Internet ermöglicht Menschen auf der ganzen Welt ohne zeitliche und räumliche Grenzen in Geschäftsbeziehungen zu treten. Der Begriff E-Commerce kann als statistisches Werkzeug zur Feststellung der Transaktionen von Gütern und Dienstleistungen über das Internet oder als Informationssystem, das online Produktkataloge zur Verfügung stellt, definiert werden (Poong, Zaman & Talha, 2006).

[3] Der Ausdruck Informations- und Kommunikationstechnik (IKT) bezieht sich auf alle technischen Mittel, die zur Datenverarbeitung und Kommunikation genutzt werden, einschließlich Computer-Hardware und -netzwerke und Software.

- **Globalisierung**: Der Cyberspace bietet neue Möglichkeiten, herkömmliche Grenzen zu überwinden;
- **Webseite Netzwerke**: Sie schaffen neue Möglichkeiten für Viktimisierung;
- **Sinoptikon und Panoptikon**: Sie schaffen mehr Möglichkeiten, potenzielle Opfer online zu überwachen;
- **Daten-Trails**: Sie schaffen neue Wege für Cyberkriminalität.

Außerdem führte das Internet zur Entstehung verschiedener Online-Umgebungen. Bei diesen handelt es sich um:

- Das **Surface Web** (Webseiten und Computer, die mit dem Internet verbunden und darüber abrufbar sind);
- Das **Deep Web** (Webseiten, die nicht über herkömmliche Suchmaschinen gefunden werden können; Intranets und medizinische Datenbanken);
- Das **Dark Web** (ein Bereich des Deep Webs, der eine attraktive Plattform für die Organisation und Abwicklung illegaler Aktivitäten bietet).

(Maimon & Louderback, 2019).

In dieser „Umgebung" kann Interaktion zwischen den folgenden Beteiligten oder Akteuren identifiziert werden, deren jeweiliges Verhalten zu Cyberkriminalität führen kann:

- **Cyberkriminelle**;
- **Komplizen** – Personen, die Cyberkriminalität unterstützen, wie Programmierer und Coder,[4] die schädliche Software[5] (Schadsoftware[6]) entwickeln, oder Händler und Verkäufer, die Mittel verkaufen/bereitstellen, mit denen Cyber-Verbrechen verübt werden können.
- **Betroffene / Opfer**;
- **Beschützer** – Polizeibehörden und Systemadministratoren.

1.2. Cyberkriminalität: von der Definition zur Typologie

In diesem Kapitel des Handbuchs werden mögliche Definitionen des Konzepts der Cyberkriminalität vorgestellt. Zum Zweck des besseren Verständnisses werden außerdem verschiedene Typologien und Kategorisierungen verwendet, um die Komplexität des Phänomens und der darin vorkommenden Handlungen zu demonstrieren.

Das **Konzept der Cyberkriminalität** bezog sich ursprünglich auf die „Computerkriminalität" und beschrieb alle Straftaten, die mithilfe von Computern oder ähnlichen Geräten, einschließlich Netzwerken und anderen Zugangsmöglichkeiten, begangen wurden. Es schloss also alle Arten von **Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Computer- und Informationssystemen und deren Ressourcen** (Hardware[7]) ein. (Gouveia, 2016 *cit in* Maia, Nunes, Caridade, Sani, Estrada, Nogueira, Fernandes & Afonso, 2016).

[4] Coder schreiben Codes, testen sie und lassen sie auf Servern laufen.

[5] Als Software werden die abstrakten Anweisungssequenzen eines Programms bezeichnet, die die Berechnungen beschreiben, die ein Computergerät durchführen soll (Councill & Heineman, 2001).

[6] Schadsoftware beschreibt schädliche Software, die für die illegale Infiltration fremder Computersysteme geschrieben wurde, um dort Schäden zu verursachen, Veränderungen vorzunehmen oder (vertrauliche oder andere) Informationen/Daten zu missbrauchen.

[7] Die internen *Hardwareteile* eines Computers werden als Komponenten (Festplatten und RAM), die externen *Hardwareteile* als Peripheriegeräte (Monitore, Tastaturen, Drucker und *Scanner*) bezeichnet.

1. CYBERKRIMINALITÄT: EINE KONZEPTUALISIERUNG

Die zunehmende Nutzung des Internets und der IKT hat die Entstehung weiterer Arten der Cyberkriminalität beschleunigt, die das Ausmaß der o. g. Angriffe auf die Verfügbarkeit, Integrität und Vertraulichkeit von Computersystemen noch übertreffen.

Dies führt zur Entwicklung weiterer Konzepte, die dem der Computerkriminalität ähneln, wie Cyberkriminalität, E-Kriminalität, und Internetkriminalität.

Aus diesem breiteren Blickwinkel betrachtet, kann Cyberkriminalität als **Kriminalität, bei der das Computernetzwerk *Ziel* oder maßgebliches *Werkzeug*** ist, definiert werden (Koops, 2010). In Übereinstimmung mit der Definition der Europäischen Kommission (2007)[8] beschreibt der Ausdruck Cyberkriminalität sowohl Straftaten, die unter Verwendung elektronischer Kommunikationsnetzwerke und Informationssysteme begangen werden, als auch Angriffe auf solche Netzwerke und Systeme.

Unter Berücksichtigung der Natur der Cyberkriminalität und der Komplexität des Konzepts erarbeiteten verschiedene Autoren Typologien oder Kategorisierungen, um das Ausmaß und die Vielfalt damit in Verbindung stehender Phänomene besser zu verstehen zu können.

Cyberkriminalität kann in zwei Kategorien unterteilt werden:

- **Cyberkriminalität im engeren Sinne** - beschreibt neue Formen von Straftaten, deren Ausführung von der Existenz und Verwendung von IKT, Computern und Computernetzwerken abhängt (Leukfeldt, Notté & Malsch, 2020; Maimon & Louderback, 2019).

- **Cyberkriminalität im weiteren Sinne** - Herkömmliche Arten von Straftaten, bei deren Ausführung IKT eine wichtige Rolle spielen, einschließlich solcher mit finanziellem Motiv, aber auch Formen der Gewalt zwischen Individuen und Sexualverbrechen. Beispiele dafür sind Cyberstalking oder Internetbetrug (Leukfeldt et al., 2020), welche im Folgenden näher ausgeführt werden.

Die Kategorisierung der Cyberkriminalität unterscheidet Straftaten, deren Ausübung direkt von Cybertechnologie abhängig ist von solchen, die durch das Internet und IKT vereinfacht werden. Letztere können weiter unterteilt werden in:

- Finanziell motivierte Cyber-Verbrechen (z. B. Phishing[9] und Romance Scam[10]);
- Cyberkriminalität in zwischenmenschlichen Beziehungen (z. B. Cyberstalking);
- Sexuelle Cyberkriminalität (z. B. Rachepornos[11]).

Die o. g. Unterteilung kann jederzeit ergänzt werden, z. B. durch Kategorien aus der folgenden Tabelle.

[8] Siehe Mitteilung der Kommission an das Europäische Parlament, den Rat und den Ausschuss der Regionen: *Eine allgemeine Politik zur Bekämpfung der Internetakriminalität*, abrufbar unter https://eur-lex.europa.eu/legal-content/DE/TXTPDF/?uri=CELEX:52007DC0267&from=DE.

[9] Weitere Informationen zu diesem Phänomen werden in Teil I, Abschnitt 1.3 dieses Handbuchs dargelegt.

[10] Weitere Informationen zu diesem Phänomen werden in Teil I, Abschnitt 1.3 dieses Handbuchs dargelegt.

[11] Weitere Informationen zu diesem Phänomen werden in Teil I, Abschnitt 1.3 dieses Handbuchs dargelegt.

Tabelle 1: Typen und Kategorien der Cyberkriminalität

Wall, 2005 *cit in* Reep-van den Bergh & Junger, 2018	**Verbrechen gegen Computer**: beschreiben unerlaubten Zugang zu Computersystemen, wie es bei Hackerangriffen oder Cracks der Fall ist[12], bei denen der Computer das Ziel des Angriffs ist (z. B. Computerviren); **Verbrechen mithilfe von Computern**: Die Verwendung von IKT, um eine Straftat zu begehen (z. B. Identitätsdiebstahl und Onlinekreditkartenbetrug); **Verbrechen „auf" Computern**, bei denen bei denen kriminelle Inhalte die Straftat sind die Straftat ist (z. B. sexueller Missbrauch von Kindern online und/oder Inhalte, die deren Ausbeutung zeigen, Androhung von Gewalt und Terrorismus).
Jahankhani et al., 2014	**Der Computer als Ziel**: zum Beispiel Diebstahl von Eigentum, unerlaubter Zugriff auf Informationen (z. B. Kundenlisten) und deren Verwendung als Drohung, um einen, auch finanziellen, Vorteil zu erlangen; **Der Computer als Instrument**: zum Beispiel die betrügerische Verwendung von Kreditkarten- und Kontoinformationen, Umwandlung oder Verschiebung von Konten, Kreditkartenbetrug; **Der Computer ist für die Ausübung der Straftat nebensächlich**: zum Beispiel Geldwäsche und illegale Finanztransaktionen; **Die Verbreitung des Computers als Voraussetzung für die Straftat**: Software-Piraterie, Urheberrechtsverletzungen im Bezug auf Computerprogramme, Fälschung von Zubehör/Programmen und Diebstahl technischer Ausrüstung.
Yar, 2006 *cit in* Jahankhani et al., 2014	**Unerlaubter Zugriff**: Das Eindringen in ein Computersystem mit dem Ziel, Eigentums- oder Besitzrechte zu verletzen (z. B. Hackerangriffe); **Onlinebetrug und -Diebstahl**: Die betrügerische Nutzung von Kreditkartendaten und (Cyber-) Geldmitteln, die durch Angriffe auf Online-Banking-Konten und E-Banking-Plattformen erlangt wurden; **Onlinepornografie**; **Gewalt im Internet**, einschließlich Cyberstalking und Hassrede im Internet; **Staatsverbrechen**, einschließlich solcher Onlineaktivitäten, die die Gesetze zum Schutz der staatlichen Integrität verletzen, wie Terrorismus, Spionage und die Veröffentlichung von Staatsgeheimnissen.

HIGHLIGHT | WICHTIGSTE INFORMATION:

Trotz der Existenz dieser und weitere Kategorisierungen gibt es keine universelle Konzeptualisierung der verschiedenen Arten der Cyberkriminalität. Ausgehend von den vorgestellten Typologien kann grob die folgende Unterteilung abgeleitet werden:

- Cyberkriminalität, die sich gegen Computer und Computersysteme richtet;
- Cyberkriminalität, die durch Computer und Computersysteme ermöglicht oder mit deren Hilfe durchgeführt wird.

Zusammenfassend lässt sich feststellen, dass Cyberkriminalität tatsächlich **eine Auswahl verschiedenster Straftaten** umfasst, bei deren Ausführung Computer entweder Mittel zum Zweck oder Ziel sind.

[12] Weitere Informationen zu diesem Phänomen werden in Teil I, Abschnitt 1.3 dieses Handbuchs dargelegt.

1.3. Arten der Cyberkriminalität: Trends

Im folgenden Abschnitt dieses Handbuchs geben wir einen kurzen Überblick über die derzeit wichtigsten (bzw. bedenklichsten) Phänomene von Cyberkriminalität. Es sollte berücksichtigt werden, dass sich Cyberkriminalität und ihre verschiedenen Erscheinungsformen, einschließlich des Kontexts, in dem sie vorkommen, der Werkzeuge, die verwendet werden und/oder ihre Ziele ständig verändern und es durchaus Aspekte der Cyberkriminalität gibt, die nicht in diesem Abschnitt des Handbuchs behandelt werden.

Trotz zunehmendem Wissen über die verschiedenen Phänomene der Cyberkriminalität steckt die Erforschung des Ausmaßes der Viktimisierung durch verschiedene Arten der Cyberkriminalität noch in den Kinderschuhen und die tatsächliche Anzahl der Betroffenen ist unbekannt (Reep-van den Bergh & Junger, 2018). Die folgenden Abschnitte stützen sich, sofern möglich, auf Daten aus offiziellen Statistiken über Cyberkriminalität, Umfragen unter Kriminalitätsopfern und/oder Studien, welche die Verbreitung der verschiedenen Arten von Cyberkriminalität messen sollen. Der Schwerpunkt liegt auf Europa.

DATEN IM FOKUS:

Die Studie von Reep-van den Bergh und Junger (2018) analysiert verschiedene Umfragen zum Thema Viktimisierung, um eine ungefähre Einschätzung der Verbreitung von Cyberkriminalität in Europa ableiten zu können.

Einige der wichtigsten Ergebnisse werden im Folgenden dargelegt:

- Zwischen 0,6 % und 3,5 % der Befragten gaben an, schon einmal Opfer von **Betrug beim Onlineshopping** geworden zu sein. In etwa 90 % der identifizierten Fälle von Cyber-Viktimisierung waren Güter oder Dienstleistungen bezahlt, aber nicht erhalten worden.
- Der Anteil von **Onlinebanking- oder Onlinezahlungsbetrug** lag zwischen 0,4 % und 2,2 %.
- Etwa 3 % der Befragten gaben an, schon einmal in der ein oder anderen Weise Opfer von **Cybermobbing** geworden oder bedroht worden zu sein. Etwa 0,6 % bis 1,0 % aller cyberkriminellen Aktivitäten entfiel auf Cybermobbing, ähnlich wie Stalking mit 0,7 % bis 1,1 %.
- **Hackerangriffe** und **Schadsoftware** stellten sich als am häufigsten vorkommende Art der Cyberkriminalität heraus: zwischen 1,2 % und 5,8 % der Befragten gaben an, schon einmal gehackt worden zu sein, und die Geräte von 2 % bis 15 % wurden bereits mit Schadsoftware infiziert.

Die Studie ist unter dem folgenden Link verfügbar: Reep-van den Bergh, C. M., & Junger, M. (2018). Victims of cybercrime in Europe: a review of victim surveys. *Crime science*, 7: 1-15.

Die o. g. Arten der Cyberkriminalität werden u. a. im Folgenden ausführlich dargelegt.

Die Probleme bei der Feststellung des Ausmaßes der Cyberkriminalität müssen berücksichtigt werden: Die Bevölkerung ist sich der verschiedenen Arten der Cyberkriminalität nicht bewusst, was dazu führen

kann, dass entsprechende Erfahrungen nicht als solche erkannt und den Behörden gemeldet werden. Des Weiteren werden einige Phänomene der Cyberkriminalität nicht angemessen ernstgenommen, was die Feststellung des tatsächlichen Ausmaßes ebenfalls erschwert (Maimon & Louderback, 2019).

1.3.1. Hackerangriffe und Cracks

Hackerangriffe oder **Cracks** sind allgemein als **unautorisierte Zugriffe auf Computersysteme mit kriminellen Absichten** definiert (Grabosky, 2016 *cit in* Maimon & Louderback, 2019). Sie werden mit dem unerlaubten Zugriff auf Computersysteme, genauer mit dem unerlaubten Übertreten unsichtbarer Grenzen von Online-Umgebungen in Verbindung gebracht. (Wall, 2001 *cit in* Maimon & Louderback, 2019).

Der Begriff Hackerangriff schließt verschiedene Handlungen mit ein, wie das **Umschreiben von Hardware- oder Softwaresystemen**, um deren ursprüngliche Funktionsweise zu verändern und das Engagement in der Hacker-Subkultur (Bachmann, 2010, Holt, 2007, Steinmetz, 2015 *cit in* Maimon & Louderback, 2019). Die Aktivität besteht aus mehreren Stufen, welche sein können: Identifizierung und Erkundung anfälliger Hardware- oder Softwaresysteme; Infiltrierung anfälliger Ziele; Änderung und Umschreibung der Zielsysteme, einschließlich der Installation von Viren oder Schadsoftware, welche bevorzugten Zugang zu Informationen und Daten ermöglichen (wie personenbezogene Daten, Passwörter/Zugangsdaten und Finanzinformationen/Bankkonten), oder sogar der Kontrolle des Systems; Verschleierung der Spuren des Eindringens und der Systemänderungen (Hughes & Delone, 2007, Wolfe et al, 2008, Holz et al., 2009, Waldrop, 2016, Luo & Liao, 2009 *cit in* Maimon & Louderback, 2019; Jahankhani et al., 2014).

Wie die meisten **Cyberverbrechen**, ermöglichen Hackerangriffe auch **die Ausführung anderer Cyberstraftaten**, wie zum Beispiel das Hacken eines E-Mail-Kontos für Cyberstalking-Zwecke (Leukfeldt et al., 2006 *cit in* Leukfeldt et al., 2020) und ein DDoS (distributed denial-of-service attack). In Bezug auf Hackerangriffe werden Hacker abhängig von ihren jeweiligen Absichten unterschieden (Furnell, 2002 *cit in* Maimon & Louderback, 2019):

- **White-Hat-Hacker** (Hacker, die sich unautorisiert Zugang zu einem System verschaffen, um dessen Sicherheit zu testen und ggf. zu verbessern);
- **Black-Hat-Hacker** (Hacker, die sich mit kriminellen Absichten unautorisiert Zugang zu Systemen verschaffen).

An dieser Stelle sollte auf eine weitere konzeptuelle Differenzierung hingewiesen werden: Die Klassifizierung des Black-Hat-Hackers ähnelt der des **Crackers**. Dabei handelt es sich um eine Person, die anders als der White-Hat-Hacker einen Nutzen aus seinem Wissen und dem unerlaubten Zugriff auf Computersysteme zieht und die Daten und Informationen, die ihm dadurch zur Verfügung stehen, für illegale Zwecke und/oder für den Zweck der Erlangung eines persönlichen oder finanziellen Vorteils einsetzt.

1.3.2. Spamming, Schadsoftware und DDoS [Distributed-Denial-Of-Service-Angriff]

Spamming oder **SPAM**, das englische Akronym für das „massenhafte Versenden von Werbematerial", beschreibt das **Senden von Daten und das massenhafte Versenden** von Werbe-E-Mails für Produkte, Dienstleistungen oder Kapitalanlagenplänen mit potenziell betrügerischem Inhalt oder sogar Schadsoftware oder anderen ausführbaren Programmdateien im Anhang (Rathi & Pareek, 2013).

Spam wird über drei Kriterien definiert:

- Anonymität – die Adresse und Identität des Absenders werden verschleiert oder fehlen;
- Massenverteilung – die E-Mail wird an eine große Anzahl Personen/elektronische Empfänger versendet;
- Unaufgefordert – der Empfänger hat die E-Mail nicht angefordert (Rathi & Pareek, 2013).

Das Ziel der Spam-Mails ist es, den Empfänger mittels Täuschung oder Lockangeboten dazu zu bringen, sich auf attraktive Produkte, Dienstleistungen oder Programme einzulassen. Der Absender verlangt z. B. Zahlungs- oder Sicherheitsdaten wie Kreditkartennummer oder andere personenbezogene Daten, bevor der Empfänger Zugang zu den Produkten oder Dienstleistungen erhält (Jahankhani et al, 2014).

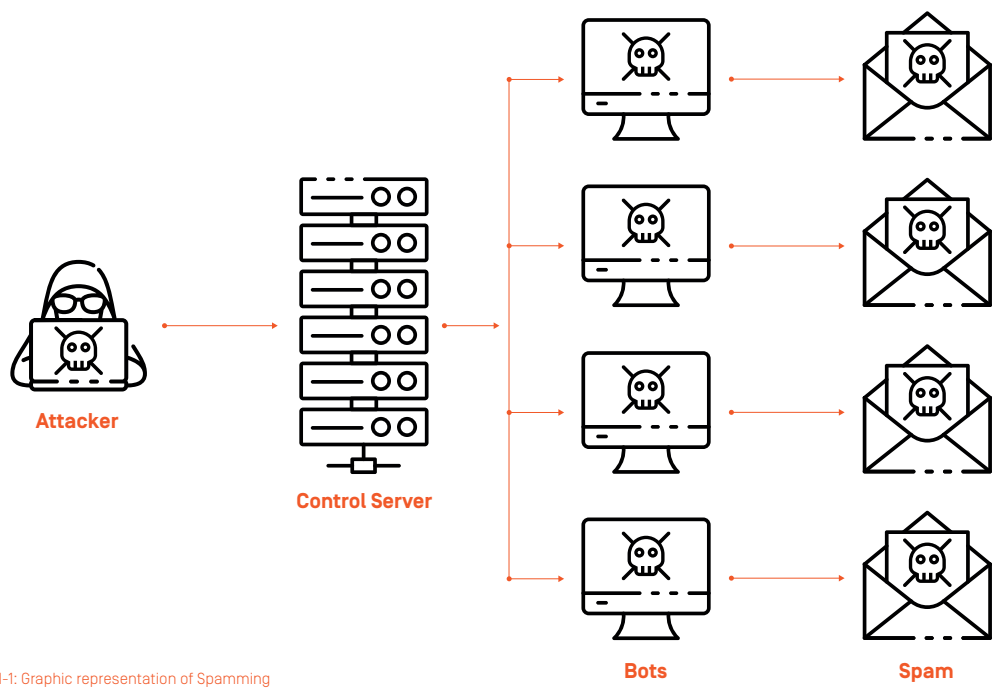


Figure I-1: Graphic representation of Spamming

Schadsoftware beschreibt verschiedene schädliche oder aggressive Arten von Software (z. B. Computerviren, Würmer,[13] Ransomware,[14] Spyware,[15] Adware,[16] Scareware[17] etc.).

Dabei handelt es sich um **Software, mit der technische Ausrüstung unerlaubt infiltriert werden kann**, um Schaden anzurichten, Änderungen vorzunehmen oder Informationen zu stehlen. Schadsoftware kann auch in Form ausführbarer Codes, Scripts, aktiver Inhalte und anderer Software auftreten (Aycock, 2006 *cit in* Reep-van den Bergh & Junger, 2018).

Häufig werden dazu Inhalte verwendet, deren Überschriften oder Betreffzeilen Neugierde wecken oder Dringlichkeit vermitteln, ebenso wie Aufforderungen zur Installation von Spielen oder Einladungen zum Besuch neuer Profile.

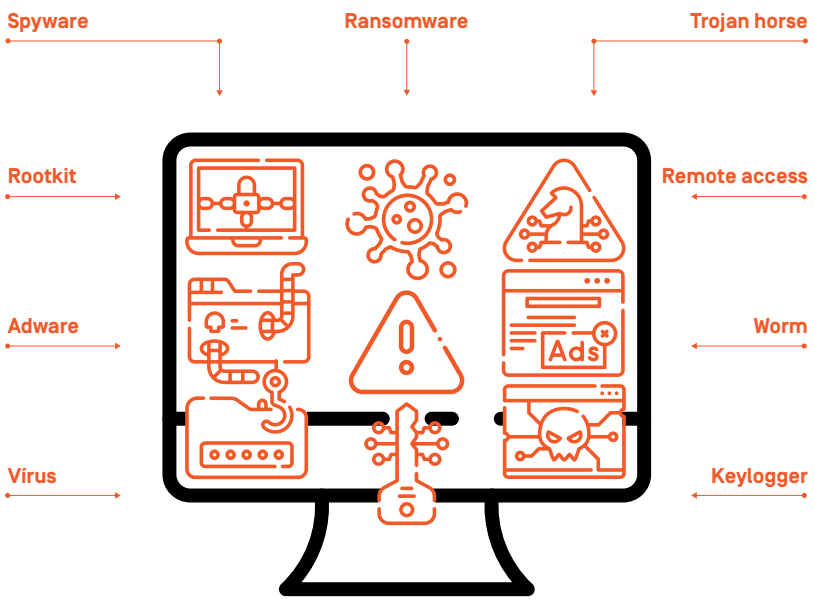


Figure I-2: Types of Malware

Ein **Distributed-Denial-Of-Service-Angriff** ist im Gegensatz dazu der absichtliche Versuch, ein spezifisches Computersystem (wie zum Beispiel das einer Regierungsbehörde oder eines großen Unternehmens) zu überlasten, um es unbrauchbar zu machen (Overvest & Straathof, 2015).

[13] Computerwürmer sind Schadprogramme, die sich mit oder ohne menschliche Hilfe in einem Netzwerk selbst vervielfältigen (Kienzle & Elder, 2003).

[14] Ransomware beschreibt Schadsoftware, die durch Herunterladen ins System gelangt und eine .exe-Datei ausführt. Das Ziel hiervon kann sein, die persönlichen Daten des Opfers zu verschlüsseln und anschließend damit zu erpressen (Kansagra, Kumhar & Jha, 2016).

[15] Spyware sind automatische Programme, die Informationen über den Nutzer und sein Surfverhalten sammeln und diese Informationen ohne das Wissen und die Einwilligung des Nutzers an Dritte weitergeben.

[16] Adware bezeichnet Software, die (in der Regel ungewollt) automatisch Werbematerial anzeigt oder herunterlädt, sobald der Nutzer online ist (Gao, Li, Kong, Bissyandé & Klein, 2019).

[17] Scareware ist eine besondere Form der Schadsoftware, die dem Nutzer vorgaukelt, sein System sei infiziert, obwohl es ordnungsgemäß funktioniert (Seifert, Stokes, Lu, Heckerman, Colcernian, Parthasarathy & Santhanam, 2015).

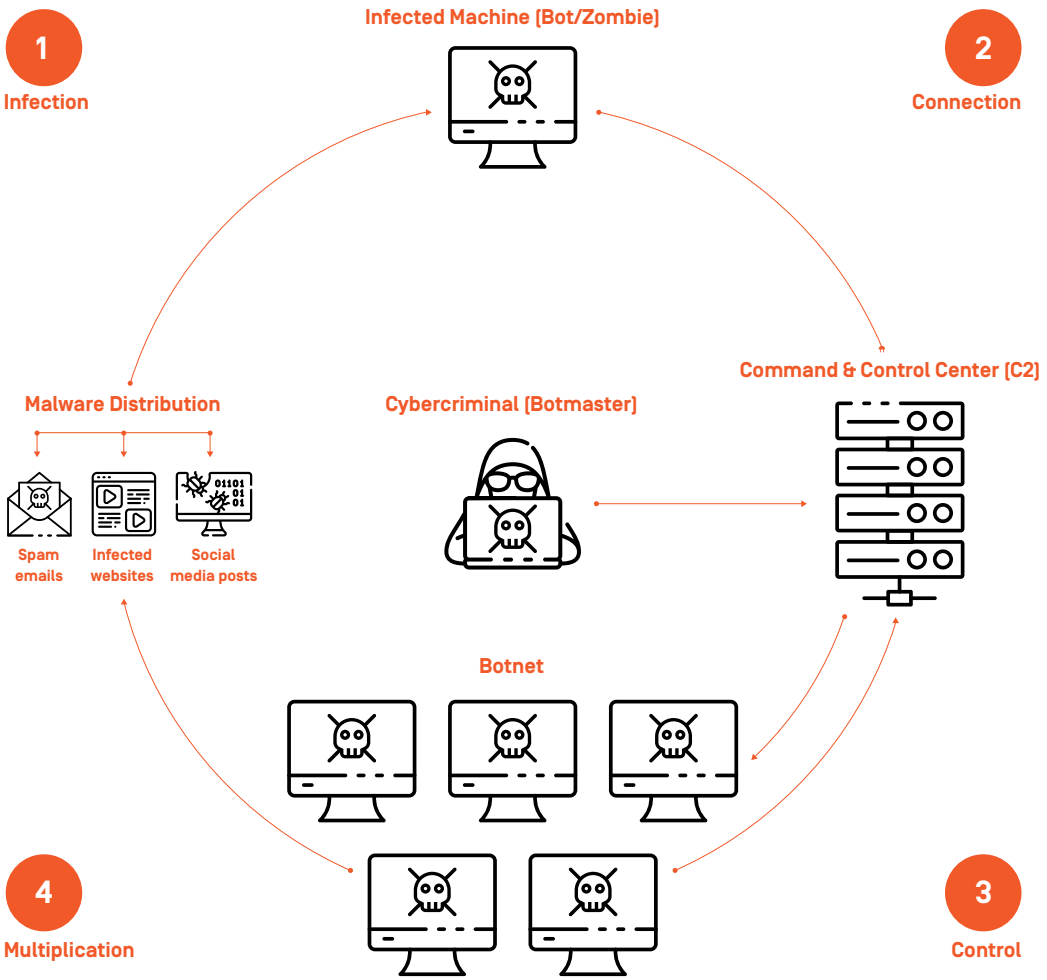


Figure I-3: Graphic representation of how a Botnet works

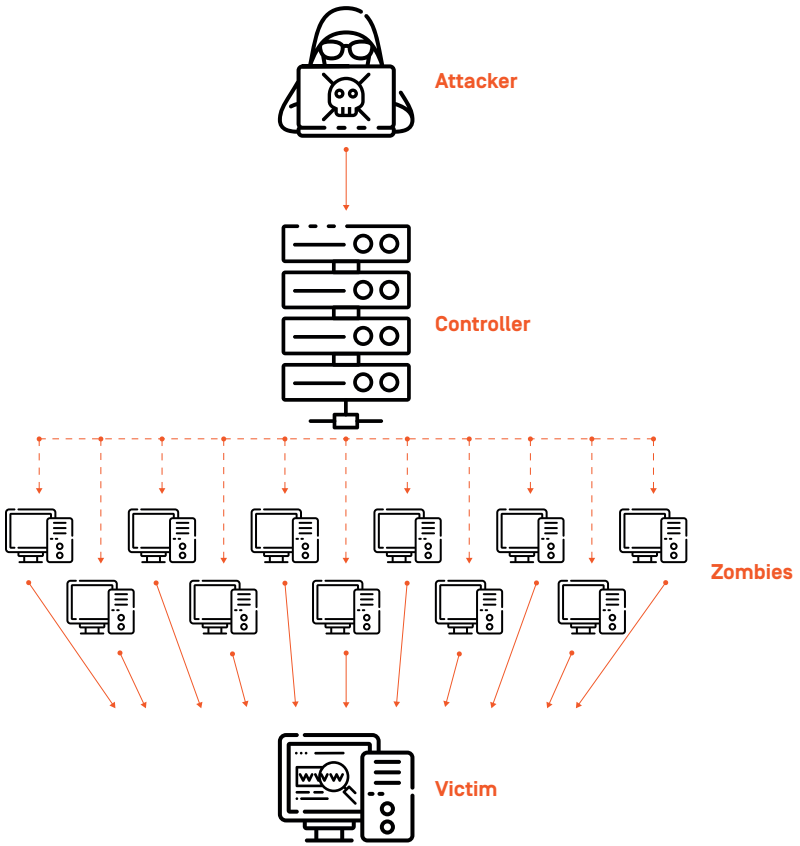


Figure I-4: : Graphic representation of a DDoS attack

1.3.3. Internetbetrug

1.3.3.1. Betrug beim Onlineshopping

Onlineshopping zeichnet sich durch die fehlende Möglichkeit zur Ansicht der Waren, Güter oder Artikel vor dem Kauf und den fehlenden direkten Kontakt zwischen den in den Kauf- und Verkaufsprozess involvierten Parteien aus (Moons, 2013, van Wilsem, 2013 *cit in* Reep-van den Bergh & Junger, 2018), was das Risiko eines Betrugs erhöht.

Betrug beim Onlineshopping tritt in **verschiedener Komplexität auf** und beginnt bei einfachen Methoden, wenn der Verkäufer dem Käufer zusichert, ihm nach der Überweisung einen Artikel zu schicken, der nie ankommt (oder es kommt ein anderer Artikel an als der, der gekauft wurde). Es gibt aber auch ausgeklügeltere Vorgehensweisen, für die häufig Dokumente wie Überweisungsscheine gefälscht werden.

Der Betrugsbegriff umfasst auch die Ausbeutung der Schwächen eines Onlineshops, der die Bankdaten seiner Kunden speichert (wie Kreditkarten- oder Kontoinformationen), auf die unerlaubt Zugriff erlangt wird und die anschließend von Cyberkriminellen im Dark Web verkauft oder für Überweisungen ohne das Wissen des Opfers verwendet werden (**Bezahlungsbetrug, engl. „card not present fraud"**). Der Diebstahl der Kontoinformationen von Nutzern für diese Art von Betrug erfolgt in der Regel durch Phishing, einem Phänomen, das in den weiteren Abschnitten dieses Handbuchs näher beleuchtet wird.

1.3.3.2. Betrug bei Online-Auktionen

Betrug bei Online-Auktionen ist eine weitere Form des Betrugs, bei der die gekauften Artikel Fälschungen sind oder illegal erworben wurden oder der Verkäufer ein nicht existierendes Produkt bewirbt oder zum Verkauf anbietet. Bei dieser Art von Betrug ist die Überweisung über Zahlungsdienstleister die bevorzugte Zahlungsmethode, da auf diese Weise die Identitäten der Beteiligten nicht offengelegt werden müssen (Jahankhani et al., 2014).

Auktions-Betrug funktioniert über Anonymität bzw. die Verwendung falscher Identifizierungsdaten bei der Registrierung auf der Auktionsplattform oder -webseite.

Die häufigsten Situationen sind:

- Erwerb/Kauf von Gütern, die der Käufer nie erhält;
- Bezahlung und Erhalt von Gütern, die nicht den gewünschten Gütern entsprechen (z. B. wenn sich das erhaltene Gut signifikant von der Beschreibung/dem Foto des Originals unterscheidet);
- Keine oder unzureichende Übermittlung relevanter Informationen über den Artikel und/oder die Verkaufsbedingungen;
- Kein Zahlungserhalt durch den Verkäufer.

1.3.3.3. Kreditkartenbetrug

Kreditkartenbetrug bezeichnet die **Nutzung der Kreditkarte einer anderen Person für persönliche Zwecke, ohne das Wissen des Karteninhabers, der Bank oder des Kreditkartenunternehmens** (Patel & Singh, 2013). Es gibt verschiedene Methoden/Straftaten, mit denen online Zugriff auf Kreditkarten oder Kreditkartendaten erlangt werden kann, darunter Phishing, E-Mail-Spam oder in Form von Hackerangriffen (Jahankhani et al., 2014).

Von den Varianten des **Kreditkartenbetrugs** ist besonders das sog. **Skimming** hervorzuheben. Dabei wird der Magnetstreifen einer Zahlungskarte ohne Wissen oder Zustimmung des Karteninhabers bei der Verwendung der Karte an einem Geldautomaten oder einem Kartenlesegerät kopiert.

Seit kurzem tritt, häufig an Geldautomaten, eine neue Form des Angriffs auf: das sog. **Jackpotting**. Diese Angriffe auf Geldautomaten erfolgen entweder durch die Einbringung einer Schadsoftware in das Computersystem des Automaten oder seiner Komponenten oder über die Verbindung mit einer Hardware, die als „Black-Box" bezeichnet wird. Dadurch können sich die Täter den Bargeldbestand des Geldautomaten auszahlen lassen.

1.3.3.4. Romance Scam und Dating-Schwindel

Als Scam werden Situationen bezeichnet, in denen der Täter versucht, eine **intime und vertrauensvolle Beziehung** zum Opfer aufzubauen, besonders über Internet und IKT, mit dem Ziel, sich **persönlich zu bereichern**.

Diese Form des Betrugs beinhaltet in der Regel:

- Erstellung gefälschter Profile in den sozialen Medien, auf Partnerbörsen oder anderen Chat- oder Austauschplattformen;
- Kontaktaufnahme mit scheinbar anfälligeren Zielpersonen;
- Eingehen einer emotionalen Bindung mit der zuvor identifizierten Zielperson;
- Entwicklung einer Hintergrundgeschichte mit der Absicht, an persönliche oder finanzielle Vermögenswerte der Zielperson zu kommen.

Der Prozess des Umwerbens und der Aufbau einer Beziehung zum Opfer zielt darauf ab, Zugang zu Geldmitteln oder anderen Vermögenswerten, Bankkonten, Kreditkarten, Reisepässen, E-Mail-Konten und/oder persönlichen Identifizierungsnummern zu erhalten. Das Ziel kann ebenso sein, das Opfer dazu zu zwingen, im Auftrag des Täters Straftaten zu begehen.

1.3.4. Identitätsdiebstahl im Internet

Identitätsdiebstahl beschreibt die **unerlaubte Erlangung personenbezogener und/oder vertraulicher Daten** eines einzelnen Opfers (z. B. Name, Ausweisnummer, Kreditkartennummer etc.) und deren **Besitz oder Übermittlung** und **Verwendung** bei der Ausübung einer Straftat (Identity Theft Resource Center, 2014).

Die Strategie besteht aus den folgenden, aufeinander aufbauenden Handlungen:

- Erlangung persönlicher und/oder vertraulicher Daten einer anderen Person ohne deren Wissen;

- Besitz oder Übermittlung solcher Daten mit dem Wissen, dass diese für illegale Zwecke eingesetzt werden;
- Nutzung zuvor erlangter Daten für das Begehen von Straftaten.

Diese Handlungen erfüllen die Kriterien des **Identitätsdiebstahls im Internet**, wenn die personenbezogenen und/oder vertraulichen Daten des Opfers über das Internet erlangt werden, und/oder wenn die erlangten Daten auf jegliche Art über das Internet übertragen werden, und/oder diese Daten für die Ausübung einer Straftat über das Internet verwendet werden.

Die Ziele sind in der Regel ein finanzieller oder anderweitiger Vorteil für den Täter oder ein Nachteil oder Verlust für das Opfer (Enisa, 2010, Harrell & Lagton, 2013, Tuli & Juneja, 2015 cit in Reepvan den Bergh & Junger, 2018), in einigen Fällen auch die Ausübung von Straftaten im Namen des Opfers. Das Opfer, dessen Identität gestohlen wurde, muss zusätzlich zum finanziellen Schaden ggf. damit rechnen, die rechtlichen Konsequenzen für die Handlungen des Täters zu tragen.

Identitätsdiebstahl an sich ist keine Straftat und kann eine Vielzahl von Vergehen, die gemäß dem portugiesischen Strafgesetzbuch definiert und strafbar sind, umfassen.

1.3.5. Phishing

Phishing bezeichnet den Massenversand von E-Mails, das sog. Spamming, die in der Regel einen Link zu einer Webseite enthalten und die Empfänger auffordern, diesen Link aufzurufen, zum Beispiel indem sie Dringlichkeit vortäuschen.

In der Regel fordern diese E-Mails den Empfänger dazu auf, seine Bankdaten zu „aktualisieren", „verifizieren" oder „bestätigen" oder weisen auf die Wichtigkeit dieser Handlungen hin.

Diese E-Mails (und die Webseiten, auf die sie weiterleiten) sind gefälscht und häufig eine ungefähre Nachbildung der echten Kundenkommunikation von Banken, Kreditinstituten oder anderen Portalen, die Onlinezahlungen ermöglichen.

Beim Zugriff auf eine solche Seite wird der Nutzer normalerweise dazu aufgefordert, Bankdaten einzugeben, damit der Straftäter diese abgreifen und missbrauchen kann.

Entsprechend besteht Phishing aus verschiedenen illegalen Aktivitäten (Jahankhani et al., 2014) und verschiedenen Phasen:

- Die Einrichtung einer gefälschten Webseite, deren Aufmachung der einer seriösen oder glaubwürdigen Organisation ähnelt, in der Regel der eines Finanzinstituts. Diese Webseite enthält ein Login- oder Registrierungsformular und kann nach Eingabe der Daten auf die echte Webseite des Finanzinstituts weiterleiten.

- Die Erstellung einer gefälschten E-Mail, die wie die Webseite das Erscheinungsbild der Kommunikation einer seriösen oder glaubwürdigen Organisation imitiert und eine dringende Handlung durch den Empfänger einfordert (z. B. eine Warnung, dass sich der Kunde umgehend einloggen muss, wenn er die Sperrung oder Deaktivierung seines Kontos/seiner Zugangsdaten verhindern will) und anschließendes Spamming.
- Erlangung personenbezogener und/oder vertraulicher Informationen über den Empfänger, einschließlich seiner Kontoinformationen, durch dessen Zugriff auf den Link.
- Missbrauch der abgegriffenen Kontoinformationen durch den Täter, um einen wirtschaftlichen Vorteil zu erlangen und/oder andere Straftaten zu begehen.

HIGHLIGHT | DATEN IM FOKUS:

Laut Eurobarometer 423[18], in dem die Wahrnehmung der EU-Bürger im Hinblick auf Internetnutzung, Cybersicherheit und Cyberkriminalität analysiert wurde, gaben 68% der Befragten an, sich Sorgen wegen **Identitätsdiebstahls im Internet** zu machen, gefolgt von Schadsoftware (66%), **Internetbetrug**, genauer: Kartenbetrug (63%), und **Hackerangriffen** auf ihre E-Mail- und Social-Media-Konten (60%).

Des Weiteren berichteten 47% der Befragten, schon einmal Ziel einer **Schadsoftware** gewesen zu sein und 31%, bereits Opfer eines **Phishing**-Angriffs geworden zu sein.

1.3.6. Sexueller Missbrauch und Ausbeutung von Kindern über das Internet

Die Weltgesundheitsorganisation (WHO) definierte 2017 sexuellen Missbrauch von Kindern als die Beteiligung eines Kindes, d. h. einer Person unter 18 Jahren, an sexuellen Handlungen:

- die das Kind nicht vollständig versteht;
- zu denen das Kind keine fundierte Zustimmung erteilen kann, oder geistig nicht in Lage ist, seine Einwilligung zu formulieren;
- die gegen geltendes Gesetz verstoßen.

Es gibt verschiedene Arten des sexuellen Missbrauchs von Kindern (WHO, 2017):

- **Berührungsloser sexueller Missbrauch**, einschließlich der Androhung sexuellen Missbrauchs, sexueller Belästigung, gezielte Kontaktaufnahme mit dem Ziel des sexuellen Missbrauchs, Aufforderung zu sexuellen Handlungen, Zeigen kinderpornografischer Inhalte und anderer Formen des Missbrauchs, die keinen direkten Kontakt zwischen Opfer und Täter erfordern;
- **Sexueller Missbrauch**, einschließlich des vaginalen, analen und/oder oralen Geschlechtsverkehrs mit dem Kind, durch einen Penis, Körperteile oder Objekte, ebenso wie

[18] Zusätzliche und ausführlichere Informationen über diesen Sonderbericht *Eurobarometer 423: Cyber security* - sind abrufbar unter https://www.europeandataportal.eu/data/datasets/s2019_82_2_423_eng?locale=en.

andere sexuelle Handlungen wie nicht angemessene Küsse, Liebkosungen und Berührungen.

Die zunehmende und immer frühere **Nutzung des Internets und sozialer Medien** durch Kinder, kombiniert mit der abnehmenden, nicht vorhandenen und/oder ineffizienten Überwachung durch die Eltern, führt zu einem zunehmenden **Risiko für sexuellen Missbrauch und Ausbeutung über das Internet** (Council of Europe, 2007 *cit in* APAV, 2019; Livingston & Smith, 2014).

DATEN IM FOKUS:

Laut der INTERPOL-Datenbank[19] *International Child Sexual Exploitation* (ICSE) wurden im Jahr 2018 über 1,5 Millionen Bilder und Videos aufgenommen und weltweit 19.400 Kinder als Opfer sexuellen Missbrauchs und Ausbeutung identifiziert.

Nach der Untersuchung einer zufälligen Auswahl von Videos und Bildern aus der o. g. ICSE-Datenbank veröffentlichten INTERPOL und ECPAT International 2018 einen gemeinsamen Bericht mit dem Titel *Towards a Global Indicator on Unidentified Victims in Child Sexual Exploitation Material in*. Wir möchten auf die folgenden Ergebnisse hinweisen:

- Bei 92 % der sichtbaren Täter handelte es sich um Männer;
- 65 % der nicht identifizierten Opfer waren Mädchen;
- Mehr als 60 % der nicht identifizierten Opfer waren noch nicht in der Pubertät, einschließlich Babys und Kleinkinder;
- Je jünger das Opfer, desto schwerer der Missbrauch;
- 84 % der Bilder enthielten explizite Inhalte sexuellen Missbrauchs von Kindern, einschließlich expliziter sexueller Handlungen.

Einige Formen des sexuellen Kindesmissbrauchs und der sexuellen Ausbeutung von Kindern über das Internet werden im Folgenden erläutert[20].

1.3.6.1. Sexueller Missbrauch von Kindern im Internet

Sexueller Missbrauch im Internet als umfassendes Konzept kann als **jegliche Form des sexuellen Missbrauchs von Kindern über das Internet** definiert werden, einschließlich verschiedener Manifestationen, von berührungslosem sexuellen Missbrauch, der durch IKT und das Internet, soziale Netzwerke und andere Plattformen erleichtert wird, wie Belästigung und Cybergrooming, bis zum Teilen von Inhalten, in denen sexueller Missbrauch oder Ausbeutung von Kindern thematisiert wird, im Dark Web (Bilder und/oder Audioaufnahmen) unter der Verwendung zuvor aufgenommener Fotografien oder Videos.

[19] Zusätzliche und ausführlichere Informationen sind abrufbar unter https://www.interpol.int/Crimes/Crimes-against-children/International-Child-Sexual-Exploitation-database.

[20] Ausführlichere Informationen über die Terminologie und die verschiedenen Formen des sexuellen Missbrauchs und Ausbeutung von Kindern finden Sie in der Übersicht *Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse* von EPCAT International und EPCAT Luxemburg, abrufbar unter http://luxembourgguidelines.org/english-version/.

1.3.6.2. Sexuelle Ausbeutung von Kindern im Internet

Das Konzept der sexuellen Ausbeutung von Kindern unterscheidet sich insofern von anderen Formen des Missbrauchs, als dass es sich durch einen Vorteil, Gewinn oder Profit auszeichnet, der dadurch entsteht, dass das Kind einer sexuellen Handlung unterzogen wird. Die Abgrenzung vom Konzept des sexuellen Missbrauchs von Kindern ist schwierig. Grundsätzlich gilt, sexuelle Ausbeutung bezeichnet die Ausbeutung der Charakteristika, Situation oder Lage des Kindes; der Gewinn wird vom Täter, Dritten oder sogar vom Kind selbst eingezogen (z. B. wenn das Kind von einem in seinem/ihrem Leben wichtigen Erwachsenen nur dann Liebe und Zuneigung erhält, wenn es sexuell missbraucht wird).

Sexuelle Ausbeutung von Kindern im Internet umfasst alle Handlungen sexueller Natur in Verbindung mit IKT, die an Kindern begangen werden, wie:

- Sexuelle Ausbeutung, während das minderjährige Opfer das Internet und IKT nutzt, einschließlich der Verführung, Manipulation und Bedrohung des Kindes zur Ausübung sexueller Handlungen, zum Beispiel vor einer Webcam;
- Identifizierung und/oder Kontaktpflege mit potenziellen Opfern im Internet zum Zweck sexueller Ausbeutung (unabhängig davon, ob die Ausbeutung und der Missbrauch online oder offline erfolgen);
- Verbreitung, Veröffentlichung, Import, Export, Angebot, Verkauf, Besitz oder bewusster Onlinezugriff auf Material, das sexuelle Ausbeutung von Kindern beinhaltet (auch wenn der sexuelle Missbrauch, der auf dem Material zu sehen oder hören ist, offline erfolgte).

1.3.6.3. Live-Übertragung sexuellen Missbrauchs von Kindern im Internet

Dieses Phänomen beschreibt die Durchführung sexueller Handlungen an Kindern und deren Live-Übertragung über Live-Streaming-Plattformen, damit sie von anderen Personen angesehen werden können. Der Zugang ist häufig zahlungspflichtig und Zuschauer haben mitunter sogar die Möglichkeit, die sexuellen Missbrauchs- und Ausbeutungshandlungen, die an den Kindern durchgeführt werden, vorzugeben oder zu beeinflussen.

Live-Übertragung bedeutet, dass Daten sofort und mit geringerem Risiko übertragen werden, da kein Datendownload erforderlich ist und das Material verschwindet, sobald die Übertragung unterbrochen wird. Dies erschwert die Untersuchung einer solchen Straftat, das Sammeln von Beweisen und die Identifizierung von Tätern und Opfern.

Live-Übertragung sexuellen Missbrauchs von Kindern im Internet beinhaltet verschiedene Formen des sexuellen Missbrauchs und der sexuellen Ausbeutung von Kindern, einschließlich der Produktion und Verbreitung entsprechender Inhalte und Prostitution. Sie stellt **eine zweifache Viktimisierung dar**: zum einen wird das Kind gezwungen oder in irgendeiner Weise aufgefordert, allein oder

zusammen mit anderen an sexuellen Aktivitäten teilzunehmen, gleichzeitig wird die sexuelle Aktivität live über IKT übertragen und an anderen Standorten von Dritten angesehen.

1.3.6.4. Cybergrooming

Cybergrooming wird als **Manipulation** und **eine Form der Verführung** von Kindern definiert. Es beginnt normalerweise mit einer platonischen Kontaktaufnahme über das Internet und IKT, einschließlich Onlinespiele und soziale Netzwerke, um eine Vertrauensbeziehung zum Kind aufzubauen und es von einem Treffen zu überzeugen, damit der Täter den sexuellen Missbrauch durchführen kann. Der Aufbau einer Vertrauensbeziehung zum Kind über das Internet und IKT kann auch darauf abzielen, das Kind zur Produktion und zum Teilen sexueller Inhalte zu bewegen[21].

Cybergrooming ermöglicht es den Tätern, sich den Opfertyp nach Belieben auszusuchen, den sie manipulieren und verführen wollen. Es bietet dem Täter viele Vorteile: Er kann eine große Anzahl Opfer gleichzeitig manipulieren, da das Internet Anonymität bietet, mit deren Hilfe er seine echte Identität verbergen und seine anderen „Identitäten", unter denen er die ausgewählten Opfer kontaktiert, verwalten kann.

Diese Form des sexuellen Missbrauchs und Ausbeutung von Kindern führt in der Regel dazu, dass der Täter das Kind durch Drohung oder Erpressung dazu bringt, die selbst produzierten sexuellen Inhalte zu verbreiten oder zu teilen, mit dem Ziel, sexuelle Gefälligkeiten, Geld oder andere Vorteile zu erlangen. Dieses Phänomen wird als sexuelle Erpressung von Kindern bezeichnet.

HIGHLIGHT | ANGEBOTE IM FOKUS:

Childline[22] ist ein kostenloses, vertrauliches Angebot speziell für Kinder und Jugendliche im Vereinigten Königreich, das sich für die Bekämpfung vieler verschiedener Schwierigkeiten und Probleme dieser Altersgruppen engagiert.

Unter anderem stellt das Programm Informationen über den sicheren Gebrauch des Internets und IKT zur Verfügung, sowie ein Online-Formular, über das das Teilen/Verbreiten selbst produzierter sexueller Inhalte gemeldet werden kann.

Das Online-Formular ist abrufbar unter: https://www.childline.org.uk/info-advice/bullying-abuse-safety/online-mobile-safety/sexting/report-nude-image-online/.

[21] Sexting zählt ebenfalls zu den selbst produzierten Inhalten sexueller Natur in Form von Texten, Bildern und/oder Videos. In der Regel werden diese Inhalte allerdings einvernehmlich und unter Gleichaltrigen geteilt. Es kann allerdings auch unter Druck oder Zwang erfolgen und sogar zur nicht-einvernehmlichen Verbreitung der produzierten Inhalte führen.

[22] Ausführliche Informationen sind abrufbar unter: https://www.childline.org.uk/.

1.3.6.5. Online-Material, das den sexuellen Missbrauch oder Ausbeutung von Kindern zeigt

HIGHLIGHT | DATEN IM FOKUS:

Laut dem o. g. Eurobarometer 423 gaben 7% der Befragten an, schon einmal versehentlich mit **Online-Material, das den sexuellen Missbrauch oder Ausbeutung von Kindern zeigt**, in Berührung gekommen zu sein.

Die Begriffe **Material, das den sexuellen Missbrauch von Kindern zeigt**, und **Material, das die sexuelle Ausbeutung von Kindern zeigt**, scheinen zumindest im nichtrechtlichen Kontext den Ausdruck Kinderpornografie (Terminologie in nationaler und internationaler Gesetzgebung) zu verdrängen und umfassen:

- Material, das den sexuellen Missbrauch von Kindern zeigt, bezieht sich auf Inhalte, in denen sexuelle Missbrauchshandlungen an Kindern und/oder deren Geschlechtsorganen dargestellt oder abgebildet werden;
- Material, das die sexuelle Ausbeutung von Kindern zeigt, bezieht sich generell auf alle Inhalte, die Kinder auf sexualisierte Art und Weise darstellen oder abbilden.

Dieser Wandel in der Begrifflichkeit wird von dem Argument gestützt, dass Material, das ein Kind auf sexualisierte Weise darstellt, eine Form sexuellen Missbrauchs von Kindern und sexueller Ausbeutung von Kindern ist und nicht als „Pornografie" bezeichnet werden sollte.

Material, das den sexuellen Missbrauch oder die sexuelle Ausbeutung von Kindern zeigt, und digital oder vom Computer generiert wurde, egal ob vollständig oder teilweise, ist ebenso als Material, das den sexuellen Missbrauch oder die sexuelle Ausbeutung von Kindern zeigt, einzustufen.

1.3.7. Cybergrooming, Cyberstalking und weitere Formen von Online-Aggressionen in zwischenmenschlichen Beziehungen

Mobbing ist ein Phänomen der Gewalt unter Gleichrangigen oder beinhaltet aggressives und gewalttätiges Verhalten durch einen Aggressor oder eine Gruppe Aggressoren gegen ein Opfer oder eine Gruppe Opfer mit dem Ziel, diese zu verletzten und ihnen Schaden oder Leid zuzufügen (APAV, 2011).

Cybergrooming beschreibt die Nutzung des Internets und IKT mit dem Ziel, das Opfer verbal anzugreifen und/oder zu seiner Ausgrenzung und sozialen Isolation beizutragen. Diese Verhaltensweisen charakterisieren diese Form der Online-Aggression unter anderem: Verbreitung schädigender/falscher Informationen mit dem Ziel, das Opfer herabzuwürdigen (über Anrufe, SMS, Videobotschaften, E-Mail, Chatrooms, Webseiten, soziale Netzwerke); Belästigung des Opfers (unter

Verwendung der gleichen Mittel) (APAV, 2011; Jahankhani et al., 2014).

Cybergrooming unterscheidet sich insofern von gewöhnlicheren Methoden des Mobbings, als dass es zu jeder Tageszeit erfolgen kann, unabhängig von der Notwendigkeit des direkten Kontakts zwischen Opfer und Täter; der Täter potenziell anonym bleiben kann; die Inhalte ein großes Publikum haben und leicht verbreitet werden können (Teilen in sozialen Netzwerken oder auf anderen Kommunikationsplattformen im Internet, in oder auf denen die Inhalte erstellt/veröffentlicht wurden und sogar auf anderen Plattformen); die erstellten Inhalte nur schwer gelöscht werden können (Stopbullying. Gov, 2017).

HIGHLIGHT | DATEN IM FOKUS:

Bei der EU-KIDS-ONLINE[23] -Umfrage über die Nutzung des Internets und Online-Verhalten und -Erfahrungen von Kindern im Alter von 9 bis 16 Jahren, die in 19 Ländern der Europäischen Union durchgeführt wurde, gaben durchschnittlich 5% der Kinder an, in den 12 Monaten vor der Umfrage **online gemobbt** worden zu sein.

In der gleichen Umfrage berichteten ca. 22% der befragten Kinder, schon einmal **Nachrichten mit sexuellen Inhalten** erhalten zu haben. Eine detaillierte Übersicht über die verschiedenen Formen sexuellen Missbrauchs und Ausbeutung von Kindern über das Internet finden Sie in den o. g. Kapiteln.

Laut den Ergebnissen der transnationalen Studie *Health Behaviour in School-aged Children*[24], die regelmäßig von der der Weltgesundheitsorganisation (WHO) durchgeführt wird, liegt der Anteil des **Cybergrooming** höher als in der o. g. Studie ermittelt: 12% der männlichen und 14% der weiblichen Heranwachsenden berichteten von Cybermobbing-Erfahrungen.

Bei den verschiedenen Formen des Cybergrooming unterscheiden wir hauptsächlich die folgenden aggressiven Verhaltensweisen im Internet mit sexuellen Motiven:

- Verbreiten von Gerüchten oder Lügen über das Sexualverhalten des Opfers;
- Verwendung beleidigender oder diskriminierender, sexualisierter Ausdrücke gegen das Opfer;
- Identitätsdiebstahl zum Zweck der Verbreitung sexueller Inhalte und/oder sexueller Belästigung von Dritten im Namen des Opfers;
- Verbreitung von Informationen über die Intimität des Opfers ohne dessen Zustimmung, zum Zweck umfassender und langfristiger Belästigung und übergriffiger Verhaltensweisen.

Abwertende Kommentare über das körperliche Erscheinungsbild einer Person im Internet oder über IKT, das sog. *Bodyshaming*, und das öffentliche Enthüllen (oder Androhen der Enthüllung) der sexuellen Orientierung oder Geschlechtsidentität einer Person ohne deren Wissen und Zustimmung im Internet oder über IKT, das sog. *Outing*, können ebenfalls als Erscheinungsformen des Cybergrooming gesehen werden.

[23] Ausführliche Informationen über die Studie finden Sie in Smahel, D., Machackova, H., Mascheroni, G., Dedkova, L., Staksrud, E., Ólafsson, K., Livingstone, S., & Hasebrink, U. (2020). *EU Kids Online 2020: Survey results from 19 countries*. EU Kids Online. Doi: 10.21953/lse.47fdeqj01ofo.

[24] Ausführliche Informationen finden Sie im Bericht über die Studie: WHO (2020). *Spotlight on adolescent health and well-being: Findings from the 2017/2018 Health Behaviour in School-aged Children (HBSC) survey in Europe and Canada - International report*. Kopenhagen: WHO-Regionalbüro Europa.

1. CYBERKRIMINALITÄT: EINE KONZEPTUALISIERUNG

Cyberstalking definiert sich als eine Form des Stalkings, die aufdringlich, wiederholend und anhaltend ist und dem Opfer Angst macht (Charakteristika dieser Form der Verfolgung und andauernder Belästigung), aber über das Internet und IKT erfolgt, mit dem Ziel, das Opfer zu bedrohen und belästigen (die Charakteristika des Stalkings(Maran & Begotti, 2019).

Cyberstalking umfasst verschiedene Tätlichkeiten: mehrere vom Opfer nicht gewollte Versuche, per Telefon, E-Mail oder soziale Netzwerke Kontakt mit ihm oder ihr aufzunehmen; Installation von Spyware auf dem Computer des Opfers; unerlaubter Zugriff auf die E-Mails und/oder Benutzerkonten in sozialen Netzwerken des Opfers, um an private Informationen zu gelangen, den Alltag des Opfers beobachten und/oder sich die Identität des Opfers anzueignen (Martellozzo & Jane, 2017).

Cyberstalking kann anderen, offline stattfindenden Formen des Stalkings vorausgehen oder sogar Teil einer Stalking- und Belästigung handlungen sein, die sowohl online als auch offline erfolgt. Täter können Personen sein, die das Opfer kennt, einschließlich Freunde und Kollegen, aber auch Ex-Partner und Unbekannte (Maran & Begotti, 2019).

HIGHLIGHT | DATEN IM FOKUS:

Im Rahmen einer europaweiten Studie über Gewalt gegen Frauen[25], für die über 40.000 Frauen aus verschiedenen Mitgliedsstaaten der Europäischen Union befragt wurde, gaben 5% an, seit ihrem 15. Lebensjahr bereits Opfer einer Form von **Cyberstalking** geworden zu sein.

Die auffälligsten Ergebnisse wurden in Schweden, mit dem höchsten Anteil von 14%, und Spanien, mit dem niedrigsten Anteil von 2%, festgestellt.

Neben Cybermobbing und Cyberstalking ist auch die **nichteinvernehmliche Veröffentlichung von Bildern und Videos** eine Form der Online-Aggression in zwischenmenschlichen Beziehungen. Dazu gehört das Teilen intimer Bilder, einschließlich Fotografien und/oder Videoaufnahmen, ohne die Zustimmung der Person, deren nackter Körper, Körperteile einschließlich Geschlechtsorganen und/oder sexueller Aktivität gezeigt wird.

Die Veröffentlichung dieser Inhalte erfolgt u. a. aus den folgenden Gründen:

- **Zwang oder Erpressung des Opfers mit sexuellen Inhalten** erfolgt, wenn der Täter damit droht, Videos und/oder Fotografien sexueller Natur, die er in der Regel einvernehmlich vom Opfer erhalten hat, zu verbreiten, sollte das Opfer nicht noch mehr Inhalte sexueller Natur produzieren oder nicht zustimmen, den Täter persönlich zu treffen.

- **Rache**, häufig auch als Racheporno bezeichnet, beschreibt die nichteinvernehmliche Veröffentlichung intimer Bilder, nämlich Fotografien, Filmen und/oder Videoaufnahmen, eines

[25] Ausführlichere, zusätzliche Informationen über die Ergebnisse der Europa-Umfrage der *European Union Agency for Fundamental Rights* sind abrufbar unterhttps://fra.europa.eu/sites/default/files/fra_uploads/fra-2014-vaw-survey-main-results-apr14_en.pdf.

Partners, als Vergeltung, in der Regel nachdem die Beziehung endete. Im Feld der Gewalt in zwischenmenschlichen Beziehungen ist die Verbreitung von Bildern und/oder Videos mit sexuellen Inhalten des früheren Partners an Familie, Freunde, über soziale Netzwerke oder sogar auf Pornoseiten nach dem Ende der Beziehung ein übliches Phänomen.

HIGHLIGHT | ANGEBOTE IM FOKUS:

In der Rubrik *Nicht ohne meine Einwilligung* bietet Facebook viele Informationen zum Thema Erpressung mit sexuellen Inhalten und nichteinvernehmlicher Verbreitung von Bildern und Videos.

Nicht ohne meine Einwilligung bietet auch die Möglichkeit, Bilder und Videos zu melden, die ohne Einwilligung geteilt oder veröffentlicht wurden, sowie eine Anleitung zum Löschen von Online-Inhalten.

Ausführliche Informationen sind abrufbar unter: https://www.facebook.com/safety/notwithoutmyconsent.

1.3.8. Weitere Formen der Cyberkriminalität

Cyberterrorismus ist eine Form des Terrorismus, bei dem Informationen, Computer, Netzwerke und technische Infrastruktur für terroristische Aktivitäten genutzt werden. Aufgrund der Wichtigkeit der verbindenden Netzwerkkomponenten könnte Cyberterrorismus sogar gefährlicher sein als *herkömmlicher* Terrorismus. Cyberterrorismus richtet sich besonders gegen Finanz- und Geschäfts- und Regierungsinfrastrukturen, Flugsicherung und medizinische Aufzeichnungen und hat den Vorteil, dass er mit wenig finanziellem Aufwand, anonym und aus der Ferne durchgeführt werden kann (Hansen, Lowry, Meservy & McDonald, 2007).

Cyberterrorismus zielt darauf ab, **die EDV-Ressourcen einer Organisation, Behörde oder der Infrastruktur stark zu beeinträchtigen und/oder lahmzulegen**: für ein Unternehmen kann ein solcher Angriff zu finanziellen Verlusten führen; eine Regierungsbehörde kann u. U. ihre Aufgaben nicht mehr erfüllen (Kratchman, Smith & Smith, 2008).

Das Konzept des Cyberterrorismus beruht auf der Zerstörung oder Lahmlegung **kritischer Infrastruktur**, deren Beeinträchtigung die nationale Sicherheit, Wirtschaft und soziale Situation des jeweiligen Landes schwächen kann (Dunn & Wigert, 2004 cit *in Yar* & Steinmetz, 2019). Zu diesen kritischen Infrastrukturen gehören Kommunikation, Energie-, Wasser-, Gesundheits- und Lebensmittelversorgung, Rettungsdienst und Katastrophenschutz sowie Symbole des nationalen Zusammenhalts (Milone, 2003 *cit in idem*). Unter diesen Infrastrukturen sind die im Informations- und Telekommunikationsbereich von herausragender Wichtigkeit, da sie für das Funktionieren der anderen kritischen Infrastrukturen eines Landes von zentraler Bedeutung sind (Dunn & Wigert, 2004 cit *in idem*).

1. CYBERKRIMINALITÄT: EINE KONZEPTUALISIERUNG

Viele der in diesem Handbuch beschriebenen Straftaten, deren Ausübung direkt von Cybertechnologie abhängt, eignen sich als Grundlage für Cyberterrorismus.

Darüber hinaus könnte man auch **Hassrede im Internet**, als Bestandteil dieses Konzepts sehen. Diese beinhaltet alle Formen der Kommunikation und Äußerungen im Internet und über IKT, die Rassismus, Fremdenhass, Antisemitismus oder andere Formen des Hasses, die auf Intoleranz gegenüber einer Person oder einer Personengruppe basiert, fördern, verbreiten, schüren oder zu rechtfertigen versuchen.

HIGHLIGHT | DATEN IM FOKUS:

Im *Flash Eurobarometer 469 - June 2018*[26] wurden die Teilnehmer zu den verschiedenen illegalen Inhalten befragt, mit denen sie online unabsichtlich in Berührung kamen. Unter anderem wurde **Hassrede** in 10 Ländern als die häufigste Art illegaler Inhalte genannt, besonders in Malta (55%), der tschechischen Republik (53%), Bulgarien (52%) und Polen (50%).

Die Teilnehmer, die angegeben hatten, mindestens eine Art illegaler Inhalte im Internet gesehen zu haben, wurden zu ihren Handlungen befragt:

- Die Mehrheit (59%) gab an, nichts unternommen zu haben, nachdem sie die illegalen Inhalte gesehen hatten.
- Unter den vorgenommenen Handlungen war die häufigste die Meldung an den Internetdienstanbieter (21%).
- Etwa eine von zehn befragten Personen kontaktierte die Person oder Organisation direkt, die für die Inhalte verantwortlich war (9%) oder alarmierte die Polizei/Behörden (8%).

Die zunehmende Nutzung des Internets, IKT und sozialer Netzwerke ging mit der Ausbreitung der **Hassrede gegen bestimmte Personengruppen im Internet** einher (Banks, 2010 *cit in* Martellozzo & Jane, 2017). Diese Ausbreitung beruht auf einigen Charakteristika des Internets und der IKT, von denen die folgenden ausschlaggebend sind (Yar & Steinmetz, 2019):

- Es ist ein billiges und effizientes Werkzeug, das keine großen finanziellen Investitionen erfordert und Hassrede potenziell einem großen Publikum zugänglich machen kann.
- Es birgt ein niedriges Risiko, gefunden und identifiziert zu werden, und bietet daher Anonymität und die Möglichkeit, die eigene Identität zu verbergen;
- Es bietet Zugang zu Kommunikationskanälen, die der Verbreitung solcher Inhalte sonst nicht zur Verfügung stünden;
- Es ermöglicht die Anpassung des Inhalts und Formats der Informationsübertragung an das Publikum und die Zielgruppen.

[26] Ausführliche Informationen sind abrufbar unter https://ec.europa.eu/digital-single-market/en/news/flash-eurobarometer-illegal-content .

HIGHLIGHT | ANGEBOTE IM FOKUS:

Im Mai 2016 veröffentlichte die Europäische Kommission in Zusammenarbeit mit vier digitalen Plattformen (Facebook, Youtube, Twitter and Microsoft) einen **Verhaltenskodex zur Bekämpfung illegaler Hassrede im Internet**[27], dem sich weitere Unternehmen anschlossen.

Eines der Ziele dieses Verhaltenskodexes ist, dass Hassrede im Internet schneller, nämlich innerhalb von 24 Stunden, gelöscht wird, um ihre Ausbreitung zu begrenzen.

1.4. Die Dunkelziffer der Cyberkriminalität

Die Zahlen bezüglich der Cyberkriminalität, die in den vorangegangenen Kapiteln dieses Handbuchs zusammengefasst sind, sprechen in ihrem Ausmaß und ihrer Bedeutung für sich, stellen die Realität aber nur unzureichend dar.

Die tatsächliche Verbreitung von Cyberkriminalität ist unbekannt. Angesichts der schwierigen Feststellbarkeit und Komplexität digitaler Beweise für Cyberkriminalität, eventueller Lücken in der Gesetzgebung und der Tatsache, dass Cyberkriminalität häufig grenzüberschreitend auftritt, gibt es höchstwahrscheinlich **viele unentdeckte, nicht gemeldete, nicht untersuchte und ungelöste Fälle von Cyberkriminalität** (Koops, 2010; Cangemi, 2004 cit in Yucedal, 2010).

Die weitverbreitete Weigerung der Opfer, Cyber-Verbrechen zu melden (Koops, 2010), sei es aus Angst, Ignoranz und/oder weil sie die Tat unterschätzen, der sie zum Opfer gefallen sind, trägt in hohem Maß dazu bei, dass das tatsächliche Ausmaß der Cyberkriminalität nach wie vor unbekannt ist.

Es gibt verschiedene Erklärungsansätze dafür, warum Cyberkriminalität nicht gemeldet wird und die daraus folgende Abweichung zwischen den Zahlen der Fälle von Cyberkriminalität, die zuständigen Behörden gemeldet werden, und der tatsächlichen Zahl der Fälle (Goucher, 2010; Kanayamaa, 2017; Maimon & Louderback, 2019; Leukfeldt et al., 2020), hauptsächlich:

- Das fehlende Wissen oder die Unfähigkeit des Opfers zu erkennen, dass er oder sie Opfer von Cyberkriminalität geworden ist;
- Scham, Schuld und Selbstvorwürfe aufgrund der Tatsache, zum Opfer von Cyberkriminalität geworden zu sein;
- Nichtanerkennung von Schäden und Verlusten, die durch Cyberkriminalität verursacht wurden;
- Widerstreben oder Weigerung des Opfers, Cyberkriminalität den zuständigen Behörden zu melden;
- Unfähigkeit, die Vorteile einer Meldung von Cyberkriminalität an zuständige Behörden zu erkennen, aufgrund der Tatsache, dass die Ermittlung fehlschlagen könnte und der Schaden, der durch Cyberkriminalität verursacht wurde, scheinbar begrenzt ist (zumindest, soweit es den

[27] Der Verhaltenskodes und weitere Informationen über dessen Erstellung und Umsetzung sind abrufbar unter https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_1135 .

Schaden des und Effekt auf den Einzelnen betrifft);
- Fehlende Kenntnis und Wissen über Cyberkriminalität seitens der Sicherheitsbehörden;
- Fehlendes Training der Sicherheitsbehörden im Hinblick auf Cyberkriminalität und fehlende finanzielle Ressourcen für weiterführende Forschung;
- Fehlende zielgerichtete und gut ausgebildete Unterstützung oder Betreuung für Opfer von Cyberkriminalität, wie es sie für die Opfer „herkömmlicher" Straftaten gibt, die dem Opfer helfen oder ihm oder ihr Zugang zu verfügbaren Ressourcen vermitteln;
- Fehlende frei zugängliche Systeme, Mechanismen (besonders online) und Meldemöglichkeiten für Straftaten der Cyberkriminalität.

Unter Berücksichtigung der gegebenen Schwierigkeiten verweisen wir in diesem Handbuch auf Beispiele für Angebote, Dienste und Mechanismen, die für die Förderung und Vereinfachung des Zugangs zu Hilfsangeboten, Informationen und Online-Mechanismen für die Meldung von Cyberkriminalität stehen.

HIGHLIGHT | ANGEBOTE IM FOKUS:

EUROPOL - Die *Agentur der Europäischen Union für die Zusammenarbeit auf dem Gebiet der Strafverfolgung* bietet auf ihrer Webseite eine Übersicht der Meldemechanismen für Cyberkriminalität (einschließlich entsprechender Online-Formulare, sofern vorhanden), die es in verschiedenen Mitgliedsstaaten gibt.

Die Seite ist abrufbar unter: https://www.europol.europa.eu/report-a-crime/report-cybercrime-online .

HIGHLIGHT | ANGEBOTE IM FOKUS:

Action Fraud ist die nationale Beschwerdeplattform für Internetbetrug und weitere Fälle von Cyberkriminalität im Vereinigten Königreich.

Zusätzlich zur telefonischen Beratung bietet Action Fraud ein Online-Meldeformular, abrufbar unter: https://reporting.actionfraud.police.uk/login .

Im Fall des **sexuellen Missbrauchs und Ausbeutung von Kindern im Internet** gibt es weitere Hürden, die die Meldung der Viktimisierungserfahrung des Kindes verhindern, wie:

- Schuld- und Schamgefühl aufgrund der Cyber-Viktimisierung, die sie erfahren haben;
- Gefühl der (Eigen-) Verantwortlichkeit aufgrund der Wahrnehmung des Opfers, dass es gewissermaßen eine Mitschuld an dem Umstand trägt, Opfer geworden zu sein;
- Angst vor Vergeltung durch den Täter und/oder Bestrafung durch rechtlich gesehen

Verantwortlichen im Fall einer Meldung;
- Angst, diskreditiert zu werden;
- Angst, die Belohnung zu verlieren, die sie vom Täter im Austausch für sexuell missbräuchliche oder ausbeutende Handlungen erhalten;
- Unvermögen, Situationen des sexuellen Missbrauchs oder Ausbeutung als illegale Handlungen zu erkennen, und/oder ihre Interpretation als Zeichen der Zuneigung.

(Goodman-Brown, Edelstein, Goodman, Jones, & Gordon, 2003 *cit in* Sigurjonsdottir, 2013; Berelowitz et al., 2012; Martellozzo & Jane, 2017; APAV, 2019).

HIGHLIGHT | ANGEBOTE IM FOKUS:

INHOPE[28] ist ein sich derzeit im Aufbau befindendes Netzwerk aus 46 *Hotlines* in verschiedenen Ländern, einschließlich der Mitgliedsstaaten der Europäischen Union, das die Bekämpfung von Online-Material, das sexuellen Missbrauch oder Ausbeutung von Kindern zeigt, zum Ziel hat.

Die Portugiesische Gesellschaft für Opferhilfe (APAV) organisiert in **Portugal** den Betrieb der Hotline für sicheres Internet [*Linha Internet Segura*], unter der Leitung des Zentrums für sicheres Internet [Centro Internet Segura], das von der Stiftung für Wissenschaft und Technologie gefördert wird. Zusätzlich zur Bereitstellung von Informationen und Unterstützung in Angelegenheiten der Cybersicherheit bietet die *Linha Internet Segura* eine Plattform, auf der **anonym illegale Inhalte im Internet einfach gemeldet werden können**. Der Schwerpunkt liegt hierbei auf Online-Material, das den sexuellen Missbrauch oder Ausbeutung von Kindern zeigt, und der Verbreitung und Unterstützung von Rassismus, Fremdenhass und anderen Formen der Gewalt,

Die Meldeplattform ist abrufbar unter: https://www.internetsegura.pt/.

In **Deutschland** gibt es mit dem *Safer Internet Center*[29] ebenfalls eine Plattform, die Familien, Kindern, Jugendlichen und Lehrern Informationen über die sichere Nutzung des Internets zur Verfügung stellt. Sie verfügt ebenso über Beratungshotlines und eine Plattform für die Meldung von Online-Material, das sexuellen Missbrauch oder Ausbeutung von Kindern zeigt: https://www.jugendschutz.net/hotline/.

Rumänien gehört ebenfalls zu den Ländern, die sich an der INHOPE-Initiative beteiligen. Dort bietet Save the Children Romania ein elektronisches Formular, das die Meldung illegaler Online-Inhalte vereinfacht. Siehe: https://oradenet.salvaticopiii.ro/esc-abuz

Im Hinblick auf **Cyberkriminalität, die sich gegen kollektive Zusammenschlüsse richtet**, nämlich große oder kleine Organisationen oder Unternehmen, deuten Studien darauf hin, dass diese weit verbreitet ist, ganz besonders **Straftaten, deren Ausübung direkt von Cybertechnologie abhängt** (Rantala, 2008 cit in Maimon & Louderback, 2019; Saini, Rao & Panda, 2012). Im Widerspruch dazu steht die geringe Anzahl gemeldeter Vorfälle, die unter anderem ihre Ursache in den folgenden Gründen haben könnte:

[28] Zusätzliche und ausführlichere Informationen sind abrufbar unter https://www.inhope.org/EN .

[29] Zusätzliche und ausführlichere Informationen sind abrufbar unter https://www.saferinternet.de/.

- Angst, den Ruf der Organisation, ihr öffentliches Erscheinungsbild und/oder die Marke, Produkte und/oder Dienstleistungen, die sie anbietet, zu diskreditieren;
- Angst, das Vertrauen der Gesellschaft und ihrer Bürger in die Aktivitäten der Organisation und deren Qualität und Verlässlichkeit zu verlieren;
- Minimierung möglicher finanzieller Verluste durch die Effekte der o. g. Gründe;
- Durchführung des Akts der Cyberkriminalität durch einen Mitarbeiter der Organisation.

2. DIE GESETZGEBUNG HINSICHTLICH CYBERKRIMINALITÄT

2.1. Cyberkriminalität nach Ansicht des Europarats

Angesichts der Notwendigkeit, Grundrechte im Cyberspace zu und die schwerwiegenden, sozioökonomischen Folgen der Cyberkriminalität zu verhindern, ist die strenge, gesetzliche Regulierung krimineller Handlungen, die hauptsächlich über Computer verübt oder durch diese vereinfacht werden, zwingend erforderlich. Die schnelle Verurteilung solcher Taten und die fortlaufende Aktualisierung der entsprechenden Gesetze dient nicht nur der Abschreckung der Täter, sondern zeigt auch, dass der Kampf gegen Cyberkriminalität von zunehmender Wichtigkeit auf der politischen Agenda der Staaten ist.[30]

Das wichtigste Instrument im Kampf gegen Computerkriminalität ist das Übereinkommen über Computerkriminalität des Europarats vom 23. November 2001, das den „Schutz der Gesellschaft vor Computerkriminalität, *unter anderem* durch die Annahme geeigneter Rechtsvorschriften und die Förderung der internationalen Zusammenarbeit" zum Ziel hat, „damit die strafrechtlichen Ermittlungen und Verfahren in Bezug auf Straftaten in Zusammenhang mit Computersystemen und -daten wirksamer werden und Beweismaterial in elektronischer Form für eine Straftat erhoben werden kann".[31] Zu diesem Zweck hält das Übereinkommen die unterzeichnenden Staaten dazu an, ihre jeweiligen materiellen und formellen Strafgesetze um die spezifischen Merkmale der Cyberkriminalität zu ergänzen, mit dem Ziel, die Gesetzgebung einschließlich Verfahrensabläufe und Beweisaufnahmeinstrumente zu vereinheitlichen und die internationale Kooperation zu vereinfachen, um die Feststellung, Untersuchung, Beweisaufnahme und Verfolgung von Cyberkriminalität zu vereinfachen. Letztendlich strebt man mit dem Übereinkommen nach der Harmonisierung der materiellen Strafgesetze und die Einführung spezifischer Verfahrensweisen, die dieser Art von Kriminalität angemessen sind, um die Verfolgung und Untersuchung durch Polizei- und Justizbehörden zu verbessern, und spricht sich für internationale Kooperation aus.

Im Hinblick auf den Schutz Minderjähriger vor sexuellem Missbrauch und Ausbeutung ist das maßgebliche Dokument das Übereinkommen des Europarats zum Schutz von Kindern vor sexueller Ausbeutung und sexuellem Missbrauch, auch bekannt unter den Namen Lanzarote-Konvention.[32] Es trat am 1. Juli 2010 in Kraft und erweiterte diverse Straftatbestände, um alle möglichen Arten sexueller Straftaten gegeben Kinder abzudecken. Eine maßgebliche Rolle bei der Verfolgung von Cyberkriminalität spielt die genaue Definition des Tatbestands des Cybergrooming, die ausdrücklich das Zeigen sexueller und illegaler Inhalte in Verbindung mit sexueller Ausbeutung und Missbrauch von Minderjährigen einschließt. Das Übereinkommen deckt zudem sexuellen Missbrauch von Kindern durch Familienmitglieder oder Vertrauenspersonen sowie Handlungen aus kommerziellen oder profitorientierten Motiven ab. Entsprechend sind die Staaten dazu angehalten, spezifische Gesetzgebung zu entwickeln, die alle in der Konvention vorkommenden Handlungen kriminalisiert, Täter einer Untersuchung zu unterziehen und strafrechtlich zu verfolgen und über Präventionsmaßnahmen im Interesse der Kinder aufzuklären. Außerdem soll die Kooperation zwischen den Staaten gefördert werden.[33]

[30] Gemeinsame Mitteilung an das Europäische Parlament und den Rat; Abwehrfähigkeit, Abschreckung und Abwehr: die Cybersicherheit in der EU wirksam erhöhen; JOIN(2017) 450 final; Brüssel, 13.9.2017; S. 2-3.

[31] Übereinkommen über Compuerkriminalität des Europarats, Budapest, 2001. https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680081561.

[32] Übereinkommen des Europarats zum Schutz von Kindern vor sexueller Ausbeutung und sexuellem Missbrauch https://rm.coe.int/protection-of-children-against-sexual-exploitation-and-sexual-abuse/1680794e97.

[33] Weitere Informationen unter https://rm.coe.int/information-note-the-council-of-europe-convention-on-the-protection-of/16807962a7.

2.2. Cyberkriminalität im Europarecht

Innerhalb der Europäischen Union (EU) wurden verschiedene Instrumente zum Kampf gegen Cyberkriminalität geschaffen. Im Jahr 2013 definierte eine Gemeinsame Mitteilung an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen die Cybersicherheitsstrategie der Europäischen Union[34]. Sie definiert die Harmonisierung der Gesetzgebung und die Umsetzung von Kooperationsmechanismen zwischen den Mitgliedsstaaten für die Sicherstellung der Cybersicherheit und Einhaltung der demokratischen Grundprinzipien der EU als Schlüsselelemente. Zu diesem Zweck fordert man die Schaffung entsprechender gesetzlicher Rahmenbedingungen für Cybersicherheit, damit wirtschaftliche und technologische Ressourcen, die die Cybersicherheit sicherstellen, aufgebaut und nationale Einheiten zum Kampf gegen Cyberkriminalität eingerichtet werden können. Die Mitteilung sieht explizit Synergien mit dem privatwirtschaftlichen Sektor vor, um digitale Resilienz zu erreichen. Des Weiteren sieht sie Präventivmaßnahmen wie Aufklärungskampagnen und gesonderte Fortbildungen zum Thema vor. Die Mitteilung fordert außerdem Investitionen in wissenschaftliche und technologische Forschung, um die technologischen Unterschiede zwischen den Mitgliedsstaaten zu überbrücken. Die Mitteilung legt fest, wie auf mögliche Cyber-Angriffe auf nachrichtendienstliche Ziele aus Nicht-EU-Staaten reagiert werden soll. Die folgenden Bereiche haben Priorität: sexueller Missbrauch von Minderjährigen, Zahlungsbetrug, *Botnets* und die unautorisierte Beeinträchtigung von Computersystemen.

Angesichts des exponentiellen Anstiegs von Cyberkriminalität in den vergangenen Jahren, verabschiedete das Europäische Parlament am 3. Oktober 2017 eine Entschließung zur Bekämpfung der Cyberkriminalität[35]. Die Entschließung „verurteilt aufs Schärfste jedweden Eingriff in Systeme, der von einem fremden Staat oder dessen Agenten vorgenommen oder gesteuert wird, um demokratische Prozesse in einem anderen Land zu stören". Außerdem betont das Europäische Parlament, dass „Sensibilisierung für die Risiken der Cyberkriminalität zwar gestiegen ist, doch die Schutzmaßnahmen einzelner Nutzer und öffentlicher Einrichtungen und Unternehmen nach wie vor völlig unzureichend sind, was in erster Linie auf mangelndes Wissen und fehlende Ressourcen zurückzuführen ist".

Die Entschließung identifiziert die Hauptsäulen im Kampf gegen Cyberkriminalität als Prävention; Sicherstellung, dass die Opfer von sämtlichen ihrer Rechte gemäß Richtlinie 2012/29/EU profitieren; Schutz der Rechte von Kindern; Stärkung der Verantwortlichkeit der Internetdienstanbieter; Verbesserung der Kooperationsmechanismen zwischen Polizei- und Justizbehörden und Internetdienstanbietern; Verfolgung einer gemeinsamen Politik im Hinblick auf ein Strafrechtssystem im Cyberspace, welche maßgeblich für die Erhebung und Erhaltung elektronischer Beweise sein wird; Stärkung der Computer- und Technologieressourcen; Verbesserung der Zusammenarbeit mit Nicht-EU-Ländern.

Die Direktiven der EU werden beständig aktualisiert, um sicherzustellen, dass sie jederzeit effektiv gegen neue Bedrohungen eingesetzt werden können. Im Folgenden finden Sie eine Liste der wichtigsten, verpflichtenden Instrumente gegen Cyberkriminalität auf EU-Ebene:

[34] Gemeinsame Mitteilung an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen; Cybersicherheitsstrategie der Europäischen Union: Ein offener, siche-rer und geschützter Cyberraum Brüssel, 7.2.2013, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52013JC0001&from=EN .

[35] Entschließung des Europäischen Parlaments vom 3. Oktober 2017 zur Bekämpfung der Cyberkriminalität (2017/2068(INI)) https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017IP0366&from=EN.

2. DIE GESETZGEBUNG HINSICHTLICH CYBERKRIMINALITÄT

Bezüglich Cyberkriminalität *im engeren Sinn*;

Richtlinie 2011/93/EU **zur Bekämpfung des sexuellen Missbrauchs und der sexuellen Ausbeutung von Kindern sowie der Kinderpornografie sowie zur Ersetzung des Rahmenbeschlusses 2004/68/JI**[36], welche als Reaktion auf neue kriminelle Phänomene in Verbin-dung mit dem sexuellen Missbrauch und der sexuellen Ausbeutung von Minderjährigen, Cyber-Grooming und Online-Kinderpornografie verabschiedet wurde. Zu diesem Zweck legt die Richtlinie Straftatbestände, Strafen und strafverschärfende Umstände fest, sowie Mindestmaße für Gefängnisstrafen, die Strafbarkeit von Versuchen und verschiedenen Formen der Urheberschaft, wie Tatbeteiligung, die Haftbarkeit juristischer Personen und die Verpflichtung zur Einrichtung von Täterdatenbanken, die Wiederholungstaten verhindern sollen. Außerdem fordert die Richtlinie die Zusammenarbeit zwischen Behörden und privaten Organisationen zum Schutz und zur Unterstützung der Opfer und die Verpflichtung zur entsprechenden Fortbildung aller am Strafverfahren Beteiligten. Diesbezüglich legt die Richtlinie besondere verfahrensrechtliche Garantien für die Opfer fest, zusätzlich zu denen der Richtlinie über die Mindeststandards der Opferrechte. Sie ruft präventive Interventionsprogramme und Präventions- sowie Interventionsmaßnahmen währen oder nach dem Strafverfahren ins Leben. Diese gesetzlichen Bestimmungen wurden im Jahr 2013 in die Gesetzgebung der Mitgliedsstaaten aufgenommen. Im Jahr 2016 wurden bereits zwei Berichte über die Umsetzung der Richtlinie in den Mitgliedsstaaten angefertigt.

Richtlinie 2013/40/EU **über Angriffe auf Informationssysteme und zur Ersetzung des Rahmenbeschlusses 2005/222/JI**[37] zielt auf die Kontrolle großangelegter Cyber-Angriffe ab und sieht vor, dass die Mitgliedsstaaten in diesem Bereich ihre nationale Gesetzgebung stärken, Straftatbestände definieren, Strafen festlegen und die Haftung juristischer Personen eindeutig festlegen. Die Richtlinie sieht außerdem die Verbesserung der Zusammenarbeit zwischen den zuständigen Behörden und Mitgliedsstaaten vor. Diese Richtlinie wurde im Jahr 2015 in die Gesetzgebung der Mitgliedsstaaten aufgenommen.

Richtlinie (EU) 2019/713 - **zur Bekämpfung von Betrug und Fälschung im Zusammenhang mit unbaren Zahlungsmitteln und zur Ersetzung des Rahmenbeschlusses 2001/413/JI**[38] ergänzt die Richtlinie 2013/40/EU und definiert digitale Handlungen, welche auf Diebstahl, Raub oder andere Formen illegaler Habhaftwerdung abzielen, Fälschung oder Verfälschung, Besitz oder Erwerb neuer, unbarer Zahlungsinstrumente als Straftaten und legt die Mindeststrafen für solche Taten fest. Diese neue Richtlinie umfasst also nicht nur Straftaten in Bezug auf materielle unbare Zahlungsinstrumente (z. B. MBway), sondern auch nichtmaterielle und elektronische Transaktionen (z. B. Transaktionen mittels virtueller Währungen). Die Definition digitaler Mittel, die in dieser Richtlinie festgelegt ist, schließt nicht nur elektronische Zahlungsmittel ein, sondern erstmalig auch Zahlungen in virtuellen Währungen.

Hinsichtlich des Sammelns und Erhaltens digitaler Beweise, besonders in Bezug auf illegale Inhalte;

Richtlinie 2000/31/EC **über den elektronischen Geschäftsverkehr**.[39] Unter den zahlreichen Inhalten

[36] Richtlinie 2011/93/EU des Europäischen Parlaments und des Rates vom 13. Dezember 2011 zur Bekämpfung des sexuellen Missbrauchs und der sexuellen Ausbeutung von Kindern sowie der Kinderpornografie sowie zur Ersetzung des Rahmenbeschlusses 2004/68/JI des Rates https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32011L0093&from=EN

[37] Richtlinie 2013/40/EU des Europäischen Parlaments und des Rates vom 12. August 2013 über Angriffe auf Informationssysteme und zur Ersetzung des Rahmenbeschlusses 2005/222/JI des Rates https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32013L0040&from=EN

[38] Richtlinie (EU) 2019/713 des Europäischen Parlaments und des Rates vom 17. April 2019 zur Bekämpfung von Betrug und Fälschung im Zusammenhang mit unbaren Zahlungsmitteln und zur Ersetzung des Rahmenbeschlus-ses 2001/413/JI des Rates https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019L0713&from=EN

[39] Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäfts-verkehrs, im Binnenmarkt ["Richtlinie über den elektronischen Geschäftsverkehr"]https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32000L0031&from=EN

der Richtlinie möchten wir besonders die hervorheben, die Dienstanbieter betreffen. Die Richtlinie legt fest, dass die Aktivität des Dienstanbieters auf den technischen Prozess des Betriebs und der Aufrechterhaltung des Zugangs zu einem Kommunikationsnetzwerk beschränkt ist, in dem die Daten Dritter übertragen oder ausschließlich zum Zweck der effizienteren Übertragung vorübergehend gespeichert werden. Entsprechend ist die Aktivität des Dienstanbieters als rein technische Aktivität zu sehen, automatisiert und passiv, was impliziert, dass der Anbieter von Diensten der Informationsgesellschaft über kein Wissen oder Kontrolle über die übertragenen oder gespeicherten Daten verfügt.

In dieser Hinsicht schafft die Richtlinie Rahmenbedingungen, in denen der Dienstanbieter nicht für illegale Inhalte, die von Nutzern über seinen Dienst geteilt werden, verantwortlich ist. Daher ist der Dienstanbieter nicht verpflichtet, die Inhalte zu überwachen und kann entsprechend nicht für diese verantwortlich gemacht werden. Dieser Haftungsausschluss wird jedoch durch die Pflicht eingeschränkt, zu handeln, wenn der Betreiber Kenntnis davon erlangt, dass die Nutzer seinen Dienst für die Speicherung illegaler Inhalte verwendet, indem er die Inhalte blockiert oder entfernt. In solchen Fällen ist der Dienstanbieter verpflichtet, umgehend nachdem er solche Inhalte entdeckt hat oder darüber informiert wurde, die Daten mit angemessener Sorgfalt zu entfernen oder den Zugang zu blockieren. Der Dienstanbieter ist nicht verpflichtet, illegale Inhalte aktiv zu überwachen; jedoch können Mitgliedsstaaten über ihre nationale Gesetzgebung Dienstanbieter zur Ermittlung und Verhinderung bestimmter Arten illegaler Aktivität verpflichten.[40]

Verordnung 679/2016 führte 2016 die **Datenschutz-Grundverordnung (DSGVO)**.[41] Dieses neue Gesetz verbessert den Schutz personenbezogener Daten. Es regelt nicht die Datenverarbeitung zum Zweck der Prävention, Untersuchung, Feststellung oder Verfolgung von Straftaten durch zuständige Behörden,[42] sondern gilt für alle anderen Situationen, in denen personenbezogene Daten verarbeitet werden, zum Beispiel wenn ein Dienstanbieter oder eine andere Organisation bei der Datenverarbeitung auf illegale Inhalte stößt und die Prüfung auf solche Inhalte nicht der Zweck der Datenverarbeitung war. Die DSGVO findet Anwendung, wenn eine Organisation personenbezogene Daten im Rahmen ihrer Aktivität erhebt und diese verarbeitet, um einer rechtlichen Verpflichtung nachzukommen, zum Beispiel[43] der Entfernung von Inhalten, die sexuellen Missbrauch oder sexuelle Ausbeutung von Minderjährigen zeigen, oder, im Fall von Finanzinstitutionen, wenn diese für den Zweck der Untersuchung, Feststellung oder Verfolgung von Straftaten gewisse personenbezogene Daten, die sie verarbeitet haben, ausschließlich den zuständigen, nationalen Behörden überlassen.

Unter den verschiedenen Bestimmungen der DSGVO erhält das in Art. 17 festgeschriebene „Recht auf Vergessenwerden" mehr Gewicht im Hinblick auf Opferrechte, besonders wenn personenbezogene Daten auf illegale Weise verarbeitet werden und so weiteren Schaden ermöglichen. Dies bezieht sich zum Beispiel auf Fälle häuslicher Gewalt, in denen Bilder oder intime Videos von einem Partner ohne das Einverständnis des Partners veröffentlicht und auf Pornoseiten Dritten zur Verfügung gestellt werden. Das Recht auf Löschung ermöglicht dem Opfer einer solchen nichteinvernehmlichen Veröffentlichung, die sofortige Entfernung der illegalen Inhalte von der Plattform einzufordern.

[40] Siehe ergänzend: Empfehlung (EU) 2018/334 der Kommission vom 1. März 2018 für wirksame Maßnahmen im Umgang mit illegalen Online-Inhalten https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018H0334&from=EN.

[41] Verordnung 679/2016, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02016R0679-20160504

[42] Vgl. Art. 2/2/d) DSGVO. In diesen Fällen ist die Sonderregelung der Richtlinie 2016/680, die durch Gesetz 59/2019 umgesetzt wurde, anzuwenden.

[43] Vgl. Art. 6/1/c) DSGVO.

Das Recht auf Vergessenwerden räumt seinem Inhaber die Möglichkeit ein, den Datenverantwortlichen **schriftlich oder mündlich** aufzufordern, die personenbezogenen Daten der betroffenen Person zu löschen. Die Umstände, unter denen dieses Recht ausgeübt werden kann, sind in Artikel 17 beschrieben.

Es muss berücksichtigt werden, dass die illegale Verarbeitung personenbezogener Daten durch den Datenschutzbeauftragten oder andere Personen/Organisationen, die nicht zur Verarbeitung Daten berechtigt sind, unter Umständen strafbar ist.[44]

Die **EU-Strategie für eine wirksamere Bekämpfung des sexuellen Missbrauchs von Kindern** 48 ist das neueste EU-Dokument hinsichtlich des sexuellen Missbrauchs und der sexuellen Ausbeutung von Kindern. Diese Mitteilung setzt ein deutliches und umfassendes Signal gegen solche Verbrechen, sowohl online als auch offline. Für den Kampf gegen solche Verbrechen legt die Strategie acht Initiativen für die Einführung und Entwicklung der passenden rechtlichen Rahmenbedingungen, die Stärkung der Strafverfolgung und die Förderung einer koordinierten Präventions-, Untersuchungs- und Unterstützungskampagne für Opfer durch verschiedenste Interessenvertreter fest und definiert spezifische Handlungsanweisungen für die Mitgliedsstaaten. Des Weiteren hält die Strategie die EU zur Schaffung eines Europäischen Zentrums für die Prävention und den Kampf gegen sexuellen Missbrauch von Kindern an, welches den Mitgliedsstaaten Unterstützung im Kampf gegen den sexuellen Missbrauch und die sexuelle Ausbeutung von Kindern bieten und die bestmögliche Koordination sicherstellen soll. Diese Strategie soll im Lauf der nächsten fünf Jahre (2020-2025) umgesetzt werden.

Auf europäischer Ebene wurden bereits Institutionen geschaffen, die die Mitgliedsstaaten im Kampf gegen Cyberkriminalität unterstützen sollen, wie zum Beispiel die *Agentur der Europäischen Union für Cybersicherheit* (ENISA), die den Austausch zwischen EU-Mitgliedsstaaten über bewährte Vorgehensweisen im Bereich der Cybersicherheit unterstützt. Bei Europol wurde 2013 eine Sonderabteilung für die Bekämpfung der Cyberkriminalität – das European Cybercrime Center (EC3) – geschaffen, um die Reaktionsfähigkeit der Strafverfolgungsbehörden innerhalb der Europäischen Union zu stärken. Das EC3 bietet den Polizeibehörden der Mitgliedsstaaten Unterstützung im Kampf gegen Cyberkriminalität in der Europäischen Union und bündelt deren Erfahrungen, um damit Untersuchungen von Cyberkriminalität zu unterstützen, die in Mitgliedsstaaten durchgeführt werden.

Zusätzlich dazu riefen die Europäische Kommission und die Vereinigten Staaten von Amerika 2012 die Global Alliance Against Child Sexual Abuse Online mit dem Ziel ins Leben, die weltweiten Bemühungen, Sexualverbrechen an Kindern im Internet effektiver zu bündeln. 54 Länder verpflichteten sich, konkrete Maßnahmen zur Verbesserung des Opferschutzes, Identifizierung und Verfolgung von Tätern, Aufklärung und Einschränkung der Ausbreitung von Kinderpornografie im Internet und der Viktimisierung von Kindern zu ergreifen.

Auf internationaler Ebene ist die Rolle der INHOPE Association hervorzuheben, deren Mission die

[44] In Portugal legt das Gesetz 58/2019 vom 8 August, Artikel 46 bis 52 die Strafbarkeit dieser Fälle fest.

Schaffung und Erhaltung von Hotlines ist, die sich dem Kampf gegen Online-Inhalte verschrieben hat, die den sexuellen Missbrauch von Kindern zeigen. Diese Hotlines fungieren auf nationaler Ebene und stehen in ständigem Kontakt mit ihren internationalen Gegenstücken, um erfolgreich eine Infrastruktur aufzubauen, die es den Mitglie-dern der Gesellschaft ermöglicht, Inhalte zu melden, die den sexuellen Missbrauch von Kindern zeigen und im Internet verfügbar sind. Die Entfernung der Inhalte und strafrechtliche Verfolgung der Täter ist das übergeordnete Ziel dieser Hotlines.

2.3. Die gesetzlichen Rahmenbedingungen hinsichtlich Cyberkriminalität in einigen Mitgliedsstaaten der Europäischen Union

2.3.1. Portugal

In Portugal bildet das am 15. September eingeführte Cyberkriminalitätsgesetz 109/2009 *Lei do Cibercrime* (LC) die Rahmenbedingungen für die strafrechtliche Verfolgung von Cyberkriminalität. Es setzt den Rahmenbeschluss 2005/222/JHA (der durch Richtlinie 2013/40/EU ersetzt wurde) um und passt die nationalen Gesetze den Beschlüssen der Budapest-Konvention (CCCE) an.

Dieses Gesetzt regelt die rechtlichen Rahmenbedingungen für Cyberkriminalität im engeren Sinn, nämlich der Verbrechen, deren Ausübung *von einem Computer abhängt*. Dieses Konzept der Cyberkriminalität betrifft Straftaten, die sich gegen Verfügbarkeit, Zugang, Integrität, Authentizität, Vertraulichkeit, Aufbewahrung und Sicherheit von Daten richten.

Es gibt jedoch andere Arten von Straftaten, die mithilfe, aber nicht ausschließlich mithilfe, elektronischer Mittel verübt werden können, die aber trotzdem Teil des Phänomens Cyberkriminalität sind. Bei einem Teil davon ist im Gesetz ausdrücklich von der Verwendung elektronischer Mittel bei der Ausübung die Rede, bei anderen wird diese nicht gesondert erwähnt. Sie können trotzdem mithilfe von Informations- und Kommunikationstechnologien (IKT) verübt werden.

Die folgenden Tabellen analysieren die in Artikel 3 bis 8 des LC definierten Straftatbestände:

2. DIE GESETZGEBUNG HINSICHTLICH CYBERKRIMINALITÄT

GESETZ ÜBER CYBERKRIMINALITÄT

Artikel und Überschrift	Tat	Art	Artikel in der Budapest-Konvention
Art. 3° - **Datenfälschung**	Die Eingabe, Modifizierung, Löschung oder Unterschlagung von Computerdaten mit der Absicht, diese in rechtlicher Hinsicht für Täuschungszwecke einzusetzen oder anderweitig die Datenverarbeitung zu stören oder falsche Daten oder Dokumente zu erstellen, mit der Absicht, dass diese für wichtige rechtliche Zwecke in Betracht gezogen oder verwendet werden, als ob sie echt wären.	Öffentlich	Art. 7
Art. 3, Paragraf 3	Die Verwendung eines Dokuments, das aus Computerdaten erstellt wurde, die in einer Handlung gemäß Paragraf 1 dieses Artikels entstanden oder die Verwendung einer Karte oder eines Geräts, auf denen Daten gespeichert sind, die im Rahmen einer Handlung nach Paragraf 1 dieses Artikels entstanden.		
Art. 4 **Beschädigung von Software oder anderen Computerdaten**	Das Löschen, Verändern, vollständige oder teilweise Zerstören, Beschädigen, Entfernen, unbrauchbar oder unzugänglich Machen von Software oder anderen Computerdaten Dritter, oder das wie auch immer geartete Beeinträchtigen deren Zugangs zu diesen Daten, ohne rechtliche Grundlage, die Einwilligung des Eigentümers oder eines anderen vollständig oder teilweise Berechtigten.	Halböffentlich	Art. 7
Art. 4, Paragraf 2	Der Versuch ist strafbar.		
Art. 5 **Computersabotage**	Das Behindern, Beeinträchtigen, Unterbrechen oder erhebliche Stören des Betriebs eines Computersystems durch die Eingabe, Übertragung, negative Beeinflussung, Beschädigung, Änderung, Löschung, Blockierung des Zugangs oder Entfernung von Software oder Computerdaten oder durch jegliche andere Form eines Eingriffs in ein Computersystem ohne rechtliche Grundlage, Einwilligung des Eigentürmers oder eines anderen vollständig oder teilweise Berechtigten.	Öffentlich	Art. 5
Art. 6 **Unerlaubter Zugriff**	Zugriff auf ein Computersystem ohne rechtliche Grundlage, Einwilligung des Eigentümers oder eines anderen vollständig oder teilweise Berechtigten.	Halböffentlich	Art. 2
Art. 6, Nr. 5	Der Versuch ist strafbar.		
Art. 7 **Unerlaubtes Abfangen von Daten**	Das Abfangen der Übertragung von Computerdaten über technische Mittel, die innerhalb eines Computersystems verarbeitet werden, an dieses System adressiert sind oder von dort versendet werden, ohne rechtliche Grundlage, Einwilligung des Eigentümers oder eines anderen vollständig oder teilweise Berechtigten.	Öffentlich	Art. 3
Art. 7, Paragraf 2	Der Versuch ist strafbar.		
Artikel 8 - **Unerlaubtes Kopieren geschützter Programme**	Das illegale Kopieren, Veröffentlichen oder Vermitteln und der Öffentlichkeit zugänglich machen eines Computerprogramms, das gesetzlich geschützt ist.	Öffentlich	
Art. 8, Paragraf 3	Der Versuch ist strafbar.		

2. DIE GESETZGEBUNG HINSICHTLICH CYBERKRIMINALITÄT

GESETZ ÜBER CYBERKRIMINALITÄT – Einstufung von Handlungen, die die Ausübung der Hauptstraftat vereinfachen oder materiell unterstützen, als eigenständige Straftaten, statt als Mitschuld.

Artikel und Überschrift	Tat	Artikel in der Budapest-Konvention
Artikel 3, Paragraf 4 - **Datenfälschung**	Kommerzieller Import, Verteilung, Verkauf oder Besitz eines Geräts, das den Zugang zu einem Computer-, Zahlungs-, Kommunikationssystem oder einem zugangsbeschränkten Dienst ermöglicht, auf das oder den die durch Paragraf 2 des Artikels verbotenen Handlungen verübt worden sind – Eingabe, Änderung, Löschung oder Unterdrückung von Daten, die auf einer Zahlungskarte oder einem anderen Gerät gespeichert oder eingebettet sind, das Zugang zu einem Zahlungssystem, Zahlungsmittel, Kommunikationssystem oder zugangsbeschränktem Dienst ermöglicht und falsche Daten oder Dokumente erstellt, mit der Absicht, dass diese für wichtige rechtliche Zwecke in Betracht gezogen oder verwendet werden, als ob sie echt wären.	Art. 6, Paragraf 1, Abs. (a) und (b)
Art. 4(3) - **Beschädigung von Software oder anderen Computerdaten**	Das widerrechtliche Erstellen, Verkaufen, Verteilen oder anderweitige Veröffentlichen oder Einschleusen von Software oder anderen Computerdaten in ein oder mehrere Computersystemgeräte, in der Absicht, unerlaubte Handlungen gemäß Paragraf 1 des Artikels auszuführen.	
Artikel 5, Paragraf 2 - **Computersabotage**	Das widerrechtliche Erstellen, Verkaufen, Verteilen oder anderweitige Veröffentlichen oder Einschleusen von Software oder anderen Computerdaten in ein oder mehrere Computersystemgeräte, in der Absicht, unerlaubte Handlungen gemäß Paragraf 1 des Artikels auszuführen.	
Art. 6, Paragraf 2 - **Unerlaubter Zugriff**	Das widerrechtliche Erstellen, Verkaufen, Verteilen oder anderweitige Veröffentlichen oder Einschleusen von Programmen, ausführbare Programmdateien, Code oder anderen Computerdaten in ein oder mehrere Computersystemgeräte, in der Absicht, unerlaubte Handlungen gemäß Paragraf 1 des Artikels auszuführen.	
Art. 7, Paragraf 3 - **Unerlaubtes Abfangen von Daten**	Das widerrechtliche Erstellen, Verkaufen, Verteilen oder anderweitige Veröffentlichen oder Einschleusen von Software oder anderen Computerdaten in ein oder mehrere Computersystemgeräte, in der Absicht, unerlaubte Handlungen gemäß Paragraf 1 des Artikels auszuführen.	

Die o. g. Artikel bedürfen einiger Überlegungen.

Artikel 3 über **Datenfälschung** stuft die Sicherheit rechtlicher Beziehungen als Gegenstand bedeutenden, öffentlichen Interesses ein, das vom Rechtsstaat sichergestellt werden muss.

Er unterscheidet sich insofern von der Definition des Computerbetrugs in Art. 221 des portugiesischen Strafgesetzbuchs, als dass er ein anderes Rechtsgut schützt. Während es sich beim **Rechtsgut** des Ersteren um die Integrität von Informationssystemen und Computerdaten handelt, schützt Letzteres rechtliche Beziehungen. Des Weiteren treffen einige Merkmale des Computerbetrugs, wie die **Erstellung gefälschter Daten oder Dokumente, mit der Absicht, diese in rechtlicher Hinsicht für Täuschungszwecke einzusetzen**

und sie wie echte Dokumente einzusetzen, noch nicht auf den Straftatbestand der Datenfälschung zu.

Wir weisen darauf hin, dass Paragraf 2 des Artikels die Fälschung von Computerdaten, die in SIM-Karten (*Subscriber Identity Module*) eingebettet sind, explizit einschließt. Dabei handelt es sich um Plastikkarten mit einem Chip (Halbleiterstruktur), auf dem digitale Informationen gespeichert werden, die es dem Inhaber erlauben, ein Mobiltelefon für den Zugang zu einem mobilen Telefonnetzwerk zu verwenden. Ziel der Straftat können ebenfalls Karten oder andere Ausrüstungsgegenstände sein, die Zugang zu einem Kabelfernsehsignal, dem Internet oder Telefonservices ermöglichen – diese fallen unter die Bezeichnung „Geräte, die Zugang zu einem zugangsbeschränkten Dienst ermöglichen".

Beispiel: Eine Phishing-E-Mail, die Josefina auf eine von Cyberkriminellen erstellte Webseite weiterleitet, die der Webseite ihrer Bank täuschend ähnlichsieht, und sie zur Eingabe ihrer Bankdaten auf dieser Seite auffordert.

Über **Artikel 4 - Beschädigung von Software oder anderen Computerdaten** will der Gesetzgeber **widerrechtliche Handlungen, die die Möglichkeit, Software oder Computerdaten zu nutzen zerstören oder beeinträchtigen**, bestrafen. Sicherheitstests an einem bestimmten System sind daher ausgeschlossen, sofern sie vom Eigentümer des Systems erlaubt worden sind.

Das geschützte Rechtsgut ist in diesem Fall die Integrität, Verlässlichkeit und vorgesehene Funktionsweise von Computerprogrammen. Im Gegensatz zu der Straftat der Beschädigung in Art. 212 des portugiesischen Strafgesetzbuchs soll Artikel 4 nicht nur Eigentum schützen, nämlich den Computer vor Schaden. Zusätzlich zur Integrität der Computerdaten als Eigentum der geschädigten Partei, schützt dieser Artikel auch **die funktionale Integrität der Daten** im Hinblick auf **die Verfügbarkeit und effektive Nutzung von Computerdaten**. Es ist keine besondere Absicht erforderlich.

Beispiel: Joãos Computer ist mit einem Virus infiziert, der seinen Computer stark verlangsamt.

Artikel 5 - Computersabotage schützt vor der **Störung von Computersystemen** oder der **Störung von Datenübertragungen**.

Die Unterscheidung zwischen Computerschaden und Computersabotage ist kompliziert. Vergleicht man beide Straftaten direkt, stellt man fest, dass der Artikel über Computerschaden Handlungen im Hinblick auf **Computerdaten** unter Strafe stellt, während der Artikel über **Computersabotage die Störung des normalen Computersystembetriebs unter Strafe stellt**. Einzeln betrachtet können computerschädigende Handlungen durch ihren Einfluss auf die Funktionsweise eines Computersystems oder einer Datenübertragung praktisch Computersabotage zur Folge haben. In diesem Fall sind **Beschädigungen lediglich eine Form des Straftatbestands der Computersabotage**. In anderen Worten, Computersabotage führt immer auch zu Computerschaden.

Das Gesetz stellt auch die Verbreitung von Viren und anderen Schadprogrammen unter Strafe, die zum Zweck der Computersabotage entworfen wurden (z. B. Art. Art. 5, Paragraf 2 LC). In diesen Fällen wird die

Vorbereitungsphase des Sabotageakts bereits kriminalisiert, zum Beispiel die Einrichtung von Botnets, über die unerlaubt Kontrolle über Netzwerke erlangt werden soll, indem ein Zombie-Computernetzwerk eingerichtet wird, dessen folgender Einsatz technische Fehlfunktionen wie DoS und DDoS verursacht.

Artikel 6 - Unerlaubter Zugriff soll die Sicherheit von Computersystemen und ihre Vertraulichkeit schützen. Dabei handelt es sich um einen abstrakten Straftatbestand, der die Verübung anderer, schwererer Verbrechen verhindern soll. Entsprechend ist bereits **der erfolgte, unerlaubte Zugriff** strafbar, da das Wissen über kommerzielle oder Betriebsgeheimnisse oder vertrauliche Daten, die gesetzlich geschützt sind, bereits strafverschärfende Umstände im Sinne der Definition des Straftatbestands des Unerlaubten Zugriffs (Art. 6, Nr. 4 LC) sind.

Keine Beschädigung oder Verlust von Daten, Programmen oder Computersystemen **ist erforderlich**, um den Straftatbestand des Unerlaubten Zugriffs zu erfüllen. Für dieses Gesetz gilt, der Zugang umfasst das Betreten des ganzen oder Teile eines Computersystems (Hardware, Komponenten, gespeicherte Daten, Dateien, Verkehrsdaten und mit Inhalten verknüpfte Daten). Allerdings stellt Art. 6.2 lediglich den Verkauf von Daten oder Programmen, die den Zugriff auf solche Systeme vereinfachen, unter Strafe, nicht aber deren Kauf.

Für die Erfüllung des Straftatbestands muss der Täter keinerlei spezifische Absichten verfolgen, die bloße Absicht, auf das System zuzugreifen ist ausreichend.

Die Straftat des Unerlaubten Zugriffs kann verübt werden durch: 1) Zugang zum System durch Ausnutzung der Schwachstellen dieses Systems oder 2) Zugang zum System durch eine dem Opfer nahestehende Person (z. B. Exfreund), die eine früher erteilte Zugriffserlaubnis missbraucht.

Beispiele: Unerlaubter Zugriff erfolgt durch eine Person, die: 1) nicht zu diesem Zugriff berechtigt ist, eine Schwäche im System ausnutzt und sich zum Beispiel Zugang zu einer privaten WhatsApp-Gruppe von High-School-Studenten verschafft und; 2) Ana verriet ihrem Freund an einem bestimmten Tag das Passwort für ihr E-Mail-Konto, damit er nachsehen konnte, ob eine wichtige E-Mail eingetroffen war. Im Wissen, dass diese Erlaubnis nur für das Prüfen der E-Mails an diesem bestimmten Tag galt, verwendete er das Passwort öfter und verschaffte sich mehrere Male Zugang zu ihren E-Mails.

Artikel 7 - Unerlaubtes Abfangen von Daten schützt das Recht auf Privatsphäre als ein Recht auf Geheimhaltung aller Computerdaten, die im Rahmen digitaler Kommunikation übermittelt werden.

Er bezieht sich nicht auf das gesetzlich erlaubte Abfangen von Daten (im verfahrensrechtlichen Rahmen, zum Beispiel gemäß Art. 12 bis 19 LC) oder das Abfangen von Daten mit der Einwilligung oder auf Anweisung der Personen, in deren Namen die Datenübertragung erfolgt (Test oder Schutzmaßnahmen mit Einwilligung der Teilnehmenden).

Das Abfangen jeglicher Form elektronischen Datentransfers via Telefon, Fax, E-Mail oder Datei ist eine Straftat. Die Straftat gilt auch **ohne die effektive Erlangung von Informationen** als begangen. Es reicht aus, mit dem Ziel zu handeln, diese Informationen zu erlangen, denn allein das versuchte Abfangen ist strafbar.

Der Ausdruck „nicht-öffentlich“ bezieht sich auf die Art der Kommunikation und nicht die Art der übertragenen Daten. Bei den übertragenen Daten kann es sich um öffentlich verfügbare Informationen handeln, aber die Parteien können vertraulich kommunizieren wollen; oder die Daten sollen aus wirtschaftlichen Gründen bis zur Bezahlung der Dienstleistung geheim gehalten werden. Entsprechend schließt der Ausdruck „nicht-öffentlich“ öffentliche Netzwerke nicht aus.

Beispiel: Pedro installiert eine Software auf Marias Handy, mit der er jederzeit Zugriff auf ihre gesamte Kommunikation hat.

Die Straftatbestände der Artikel 3 bis 7 schließen mit dem gleichen Strafmaß die Erstellung, den Verkauf, die Verteilung, Veröffentlichung oder Platzierung eines Geräts oder Programms in einem Computersystem, die die Verübung der Straftat ermöglichen, mit ein. Z. B.: Im Fall eines Unerlaubten Zugriffs gilt derjenige als Täter, der das Programm geschrieben hat, welches einem Dritten Zugang zum System einer weiteren Person erlaubte, auch wenn der Täter auf dieses System nicht selbst zugegriffen oder den Zugriff versucht hat.

Artikel 8 - Unerlaubtes Kopieren geschützter Programme schützt die Urheber- und Nutzungsrechte, z. B. an einem Computerprogramm. In diesem Sinne legt Artikel 14 der DL 252/94 von 20/10, der den rechtlichen Schutz von Computerprogrammen definiert, ausdrücklich fest, dass die Bestimmungen des Artikels 9(1) LC bei Computerprogrammen Anwendung finden. Man geht davon aus, dass der Staat ausdrückliches Interesse am **Schutz des Urheberrechts** hat und die strafrechtliche Verfolgung von Verstößen gegen solche Rechte daher im Interesse des Staates liegen und gerechtfertigt sind. Entsprechend bedarf diese Straftat keiner Anzeige, da öffentliches Interesse vorliegt.

Die Artikel 11 bis 19 legen verfahrensrechtliche Bestimmungen fest, die das umgehende Sammeln und Erhalten elektronischer Beweismittel erlauben. Sie gelten also auch für die Straftaten, die in diesem Gesetz festgeschrieben sind, die mithilfe eines Computersystems verübt werden oder die einer Beweisaufnahme in elektronischer Form bedürfen.

Die Artikel 20 bis 26 betreffen die internationale Zusammenarbeit und Artikel 27 legt die Zuständigkeit fest.

Das portugiesische Strafgesetzbuch und dessen Bestimmungen im Hinblick auf Cyberkriminalität

Wie bereits erwähnt finden sich in der portugiesischen Gesetzgebung zusätzlich zum LC weitere Straftatbestände, die unter anderem mithilfe von elektronischen Mitteln verübt werden können und als Cyber-Verbrechen bezeichnet werden.

In einigen Fällen legt das Gesetz ausdrückliche Bestimmungen für die Verwendung solcher elektronischen Mittel fest, in anderen nicht. Im Strafgesetzbuch selbst gibt es Bestimmungen, die sich ausschließlich auf die Verwendung elektronischer Mittel zur Ausübung der Straftat beziehen. Die folgende Tabelle gibt einen Überblick über die Bestimmungen bezüglich Cyber-Verbrechen:

2. DIE GESETZGEBUNG HINSICHTLICH CYBERKRIMINALITÄT

PORTUGIESISCHES STRAFGESETZBUCH

Artikel und Überschrift	Tat	Art
Artikel 152, Paragraf 2, Abs. b] - **Häusliche Gewalt**	Die Verbreitung persönlicher Daten wie Bilder oder Audioaufnahmen eines der Opfer über das Internet oder andere Mittel allgemeiner Veröffentlichung ohne dessen Zustimmung, die dessen Privatsphäre verletzen.	Öffentlich
Art. 176, Paragraf 1, Abs. a], b], c] und d] - **Kinderpornografie**	Der Einsatz eines Minderjährigen in pornografischen Inhalten oder dessen dahingehende Beeinflussung; der Einsatz eines Minderjährigen in pornografischer Fotografie, Filmen oder Aufnahmen, unabhängig vom Medium, oder die Beeinflussung des Minderjährigen zur Teilnahme; Produktion, Verbreitung, Import, Export, Weitergabe, Ausstellung, *oder Bereitstellung*[46] von Inhalten wie in den o. g. Paragrafen beschrieben; Kauf, Speicherung oder *Besitz*[47] solcher Inhalte mit dem Ziel, diese zu verbreiten, importieren, exportieren, weiterzugeben, auszustellen oder bereitzustellen.	Öffentlich
Art. 176, Nr. 5	Der Kauf, Besitz, Zugang, die Erlangung oder das Zugänglichmachen der in [b] dargelegten Inhalte durch ein Computersystem oder jegliche andere Mittel.	
Art. 176, Nr. 6	Die Teilnahme an, Unterstützung oder *Bereitstellung*[48] pornografischer Inhalte mit Minderjährigen unter 16 Jahren, entweder persönlich, über ein Computersystem oder durch jegliche andere Mittel.	
Art. 176, Nr. 8[45]	Der Versuch ist strafbar.	
Art. 176 - A – **Cyber-Grooming Minderjähriger**	Die gezielte Kontaktaufnahme Erwachsener mit Minderjährigen über Informations- und Kommunikationstechnologien, in der Absicht, Minderjährige sexuell zu missbrauchen oder Kinderpornografie anzufertigen.	Öffentlich
Art. 193 – **Eingriff in die Privatsphäre mithilfe von IKT**	Die Erstellung, Speicherung oder Verwendung individuell identifizierbarer, personenbezogener Daten über politische, religiöse oder philosophische Einstellungen, Partei- oder Gewerkschaftszugehörigkeit, Privatleben oder ethnische Herkunft.	Öffentlich
Art. 193, Paragraf 2	Der Versuch ist strafbar.	
Art. 221 - **Computer- und Kommunikationsbetrug**	Störung des Ergebnisses der Datenverarbeitung oder fehlerhafte Strukturierung eines Computerprogramms durch unvollständige oder falsche Daten, externe Daten oder jegliche andere Art der unerlaubten Störung mit der Absicht, sich selbst oder einen Dritten unrechtmäßig zu bereichern und einer anderen Person Schaden zuzufügen.	Halböffentlich
Art. 221, Paragraf 2	Das Eigentum anderer mittels Programmen, elektronischen Geräten oder anderen Mittel, die entweder einzeln oder in ihrer Gesamtheit dazu gedacht sind, ganz oder teilweise den normalen Betrieb oder Betrieb von Telekommunikationsdiensten zu stören, verändern oder verhindern.	
Art. 221, Paragraf 3	Der Versuch ist strafbar.	
Verbrechen und Vergehen werden heutzutage meistens mithilfe elektronischer Mittel durchgeführt, auch wenn deren Verwendung nicht ausdrücklich im Gesetz erwähnt wird;		
Art. 154a - **Schikane**	Die wiederholte Verfolgung oder Belästigung einer Person auf jegliche Art und Weise, direkt oder indirekt, die Angst oder Beunruhigung hervorruft oder deren Urteilsfähigkeit beeinträchtigt.	Halböffentlich

[45] Die Überarbeitung von Nr. 8 des Artikels 176 des Gesetzes Nr. 187/XIV/1 ergänzt eine Definition der „pornografischen Inhalte" als jegliche Inhalte, die sexuellen Zwecken dienen und echte oder nachgestellte, explizite, sexuelle Handlungen Minderjähriger oder Abbildungen ihrer Sexualorgane oder anderer Körperregionen beinhal-ten.

[46] „oder Bereitstellung" - Änderung durch Gesetz Nr. 187/XIV/1 des Artikels 176, Nr. 1 CP.

[47] „Oder Besitz " - Änderung durch Gesetz Nr. 187/XIV/1.ª bis Abs. d] des Artikels 176, Nr. 1 CP.

[48] „Bereitstellung" - Änderung durch Gesetz Nr. 187/XIV/1 für Nr. 6 des Artikels 176 CP.

Art. 154a, Paragraf 2	Der Versuch ist strafbar.	
Art. 192 – **Eingriff in die Privatsphäre**	Das Abfangen, Aufzeichnen, Verwenden, Übertragen oder Weitergeben einer Unterhaltung, eines Telefongesprächs, E-Mail-Verkehrs oder von Rechnungsunterlagen; das Erfassen, Fotografieren, Filmen, Aufzeichnen oder Weitergeben von Fotos von Personen, Objekten oder Privaträumen; das heimliche Beobachten oder Belauschen von Personen, die sich in deren Privaträumen befinden oder das Verbreiten von Informationen in Zusammenhang mit dem Privatleben oder einer ernsthaften Erkrankung des Opfers ohne dessen Zustimmung und mit der Absicht, in die Privatsphäre des Opfers einzudringen, besonders im Hinblick auf deren familiäre oder sexuelle Intimität.	Halböffentlich
Artikel 194 - **Bruch des Brief- oder Kommunikationsgeheimnisses**	Das Öffnen eines Pakets, eines Briefs oder eines anderen Schriftstücks, das sich in einem verschlossenen Umschlag befindet, das nicht an einen selbst adressiert ist, oder die Erlangung von Wissen über dessen Inhalt durch technische Prozesse, oder die wie auch immer geartete Verhinderung der Zustellung; die Beeinträchtigung des Inhalts einer Telekommunikationsübermittlung oder die Erlangung von Wissen über diese Inhalte und die Veröffentlichung des Inhalts von Schriftstücken in verschlossenen Umschlägen oder Telekommunikationsübermittlungen.	Halböffentlich
Artikel 199 - **Unerlaubte Aufnahmen und Fotografien**	Das Aufnehmen gesprochener Worte einer anderen Person, die nicht für die Öffentlichkeit bestimmt sind, ohne deren Zustimmung, selbst wenn diese Worte an einen selbst gerichtet sind; die Verwendung oder Erlaubnis der Verwendung solcher Aufnahmen, auch für den Fall, dass die Aufnahmen nach geltendem Recht gemacht wurden; das Fotografieren oder Filmen einer anderen Person, auch bei Veranstaltungen, an denen rechtmäßig teilgenommen wurde oder die Verwendung oder Erlaubnis der Verwendung solcher Fotografien oder Filme, wie eingangs erwähnt, auch für den Fall, dass die Aufnahmen nach geltendem Recht gemacht wurden.	Halböffentlich
Art. 199, Paragraf 2, b)	Unautorisierte Veröffentlichung von Bildern.	
Art. 240(1)(a) und (b) - **Diskriminierung und Anstiftung zu Hass und Gewalt**	Die Einrichtung oder Gründung einer Organisation oder die Teilnahme an organisierten Propaganda-Aktivitäten, die Diskriminierung, Hass oder Gewalt gegen Personen oder Gruppen von Personen aufgrund deren Rasse, Hautfarbe, ethnischer oder nationaler Herkunft, Abstammung, Religion, Geschlecht, sexueller Orientierung, Geschlechteridentität oder körperlicher oder geistiger Behinderung unterstützen oder dazu aufrufen; oder die aktive Unterstützung der Organisation oder Teilnahme an deren Veranstaltungen, wie im o. g. Unterabschnitt beschreiben, einschließlich finanzieller Unterstützung.	Öffentlich
Art. 240, ff. 2, al) a	Die öffentliche oder über jedwede Kanäle zur Veröffentlichung gedachte Provozierung von Akten der Gewalt, Diffamierung, Beleidigung, Bedrohung oder Anstiftung zu Gewalt oder Hass gegen Personen gemäß Paragraf 1 durch die Rechtfertigung, Leugnung oder grobe Verharmlosung von Völkermordverbrechen, Kriegsverbrechen oder Verbrechen gegen den Frieden und die Menschlichkeit.	

Die Bestimmung des **Artikels 152, Paragraf 2, b) - Häusliche Gewalt** wurde durch Gesetz 44/2018 eingeführt. Die neue Vorgabe soll besonders intime (nämlich sexuelle) persönliche Daten (nämlich Bilder und Audioaufnahmen, einschließlich Videos, Filme, Fotos) und die Privatsphäre der Opfer schützen, wenn solches Material ohne die Zustimmung des Opfers über das Internet oder andere Mittel groß angelegter öffentlicher Verbreitung (z. B. soziale Netzwerke) veröffentlicht (gepostet/

verbreitet) werden. Durch diese Spezifizierung soll Cyberstalking im Kontext häuslicher Gewalt härter bestraft werden können (laut Carolina Villacampa Estiarte als eine Straftat, die hauptsächlich aus „dem Senden aggressi-ver oder bedrohender E-Mails, Textnachrichten und Sofortnachrichten, dem Veröffentlichen gemeiner Kommentare über das Opfer im Internet, das Teilen intimer Fotos oder Videos des Opfers über das Internet" bestehen, die als „stärkerer Eingriff in die Privatsphäre des Opfers" wahrgenommen werden und die „sich in psychologischer Hinsicht nachteiliger auswirken").

Die Liste der verbotenen Materialien in **Artikel 176 - Pornografie Minderjähriger** ist detaillierter als die der Richtlinie 2011/93/EU, wenn auch nicht so gründlich wie die Lanzarote-Konvention. An dieser Stelle sei darauf hingewiesen, dass der Gesetzentwurf Nr. 187/XIV/1 einige Paragrafen dieses Artikels ergänzte (s. Fußnote zur Tabelle) und den Artikel 176-B hinsichtlich der Organisation von Reisen, deren Ziel der Sextourismus mit Minderjährigen ist, zum Strafgesetzbuch hinzufügte.[49]

Artikel 176 - Verführung Minderjähriger für sexuelle Zwecke wurde dem Strafgesetzbuch am 24. August durch Gesetz Nr. 103/2015 hinzugefügt. In Übereinstimmung mit der Richtlinie 2011/93/EU wurden neue Formen des sexuellen Missbrauchs und der sexuellen Ausbeutung via IKT unter Strafe gestellt, wie zum Beispiel Cyber-Grooming Minderjähriger, pornografische Handlungen in Echtzeitübertragung oder der wissentliche und absichtliche Zugriff auf kinderpornografische Inhalte auf bestimmten Internetseiten.

Artikel 193 – Eingriff in die Privatsphäre mithilfe von IKT leitet sich von Artikel 35(3) der Verfassung der Portugiesischen Republik ab. Er soll Persönlichkeitsrechte vor möglicher Diskriminierung schützen, deren Gefährlichkeit durch den Einsatz von Computern exponentiell gesteigert wird. Daher bedarf eine strafrechtliche Verfolgung einer Straftat gemäß Artikel 193 keiner Anzeige als Grundlage. Es handelt sich um ein Offizialdelikt, dessen Verfolgung grundsätzlich im Interesse und der Verpflichtung des Staates liegt. Der Straftatbestand des Eingriffs in die Privatsphäre mithilfe von IKT umfasst nicht nur das Anfertigen unrechtmäßiger Dateien des geschützten Guts, sondern auch deren Speicherung und Verwendung, selbst, wenn man nicht an deren Anfertigung beteiligt war. Die Definition des Verbrechens ist möglichst breit angelegt, um als Abschreckung dienen zu können, da der Nachweis des tatsächlichen Urhebers des Materials häufig schwierig ist. Entsprechend ist auch der Versuch strafbar.

Die Kriminalisierung von **Computer- und Kommunikationsbetrug** gemäß **Artikel 221** orientiert sich an den allgemeinen Entwicklungen im Bereich des Betrugs und teilt die Tatmerkmale des Artikels 217 Strafprozessordnung – die Absicht, sich selbst oder einen Dritten widerrechtlich zu bereichern und dem Opfer Schaden zu verursachen. Wie auch bei der Straftat des Betrugs ist hier der Versuch strafbar und die strafrechtliche Verfolgung bedarf einer Anzeige. Die Besonderheit dieses Vergehens liegt im Vorgehen: der Verwen-dung von IKT, z. B. der arglistigen Verwendung von Computertechnologie zur Manipulation von Daten oder Ergebnissen. Paragraf 1 des Artikels bezieht sich auf die Beeinflussung von Datenverarbeitungsergebnissen, um einen illegalen Vorteil zu erhalten, während sich Paragraf 2 auf den Einsatz von IKT zur Störung der Integrität oder des Normalbetriebs eines Computersystems zur Erlangung eines illegalen Vorteils bezieht.

[49] Zum Zeitpunkt der Veröffentlichung dieses Handbuchs sollte dieser Gesetzentwurf bereits vom Parlament ver-abschiedet worden sein und kurz vor der öffentlichen Bekanntmachung stehen. Entsprechend werden die Än-derungen als sicher angesehen, aber der Name und die Nummer des Gesetzes können noch nicht angegeben werden. Vgl. https://www.parlamento.pt/ActividadeParlamentar/Paginas/DetalheIniciativa.aspx?BID=44369

2. DIE GESETZGEBUNG HINSICHTLICH CYBERKRIMINALITÄT

Jetzt sollen die Vorschriften hinsichtlich der Straftaten analysiert werden, bei denen IKT durch die exponentiell steigende Verwendung von Internet und Smartphones im Allgemeinen am wahrscheinlichsten verwendet werden, auch wenn der Straftatbestand die Verwendung von IKT nicht explizit nennt.

Bei **Artikel 194 - Bruch des Brief- oder Kommunikationsgeheimnisses** entspricht die Verbreitung der Inhalte über das Internet einem strafverschärfenden Umstand (vgl. Art. 197 CP). Dieser Artikel leitet sich aus Artikel 34 der portugiesischen Verfassung ab, dem grundlegenden Recht auf Geheimhaltung der Kommunikation, und definiert dessen Bruch als Straftat. Es findet in Bezug auf elektronische Korrespondenz (E-Mail) und alle anderen Arten elektronischer Kommunikation und Mobiltelefondienste (SMS etc.) Anwendung, die eine moderne Entsprechung von geschlossener, postalischer Konferenz sind. Die Vorschrift schützt die Rechtsgüter Privatsphäre, Schutz der freien Meinungsäußerung und Vertrauen in die Integrität von Kommunikationsmitteln, nämlich Telekommunikationsdienste und deren Sicherheit.

Der Schutz umfasst sowohl den Inhalt der elektronischen Kommunikation als auch die Umstände der Übermittlung (Verkehrsdaten). Das bloße Speichern von Daten stellt einen Bruch dar, der sich bei jeder neuen Verwendung der Inhalte der Verkehrsdaten wiederholt. Im Fall elektronischer Kommunikation ist der Straftatbestand bereits mit dem Zugriff erfüllt, es muss keine Kenntnis des Inhalts erlangt werden (es ist nicht notwendig, die Nachricht zu „öffnen").

Hier stellt sich die Frage, ob diese Straftat nicht vom Straftatbestand des unerlaubten Abfangens von Daten gemäß Artikel 7 Gesetz 109/91 abgedeckt ist. Unserer Meinung nach gibt es zwischen den Gesetzen in dem Moment eine Überschneidung, wenn die Nachricht während der Übertragung abgefangen wird, aber diese ist nicht länger gegeben, wenn der Zugriff erfolgt, nachdem die Nachricht vom Empfänger empfangen und in dessen elektronischem Postfach gespeichert wurde. Letzteres könnte als unerlaubter Zugriff gemäß Artikel 6 LC angesehen werden. Wir sind jedoch der Meinung, dass eine solche Interpretation nicht möglich ist, da dieser Straftatbestand ein **Motiv** erfordert: **„die Absicht, für sich selbst oder einen Dritten einen illegalen Vorteil zu erlangen"**, die kein Merkmal der Straftat des „Bruchs des Brief- oder Kommunikationsgeheimnisses" ist. Es kann also nicht gerechtfertigt werden, dass eine elektronische Nachricht, sobald sie empfangen wurde, weniger geschützt ist als ein Brief. Unserer Meinung nach bezieht sich die Definition dieses Verbrechens auch auf elektronische Post.

Der Schutz der Privatsphäre und Persönlichkeitsrechte umfasst auch die folgenden Straftaten: **Einbruch oder Verletzung des Hausrechts** (Art. 190 Strafgesetzbuch), Hausfriedensbruch (191 Strafgesetzbuch), **Verletzung der Privatsphäre** (Art. 192 Strafgesetzbuch), **Verstoß gegen Geheimhaltungspflicht** (Art. 195 Strafgesetzbuch). Die Verbreitung der Inhalte über das Internet wirkt sich in jedem dieser Fälle strafverschärfend aus, vgl. Art. 197 Strafgesetzbuch).

Die Bestimmung bezüglich der **Anfertigung illegaler Aufnahmen und Fotografien** gemäß **Art. 199 des portugiesischen Strafgesetzbuchs** schützt das Recht am eigenen Bild. Der Verstoß dagegen

ist eine rechtlich eigenständige, strafbare Handlung, unabhängig von der Privatsphäre oder Intimität der oder des Dargestellten. Das Recht am eigenen Bild deckt zwei eigenständige Rechte ab: das Recht, nicht fotografiert zu werden, und das Recht auf Nicht-Veröffentlichung der Aufnahmen. Die betroffene Person kann einwilligen, fotografiert zu werden, aber die Einwilligung in die Veröffentlichung der Aufnahme verweigern. Niemand darf gegen seinen Willen fotografiert werden, noch dürfen die Aufnahmen ohne ausdrückliche Einwilligung verwendet werden.

Beispiel: João hat mit Marias Einwilligung ein Foto von ihr gemacht. Dieses Foto veröffentlich er gegen ihren Willen auf *Facebook*.

Zusätzlich können weitere Straftaten begangen werden, deren Auswirkungen durch die Verwendung von Technologie verstärkt werden. **Hierbei handelt es sich um Straftaten, deren Typologie nicht die Verwendung von Technologie als bestimmendes Merkmal enthält**.

Stalking gemäß **Art. 154-A** kann über elektronische Mittel begangen werden: Cyberstalking. Cyberstalking erfolgt über einen längeren Zeitraum, in dem sich die Auswirkungen häufig intensivieren. Stalking geht oft mit anderen Straftaten einher, wie z. B. Art. 193 Strafgesetzbuch, Eingriff in die Privatsphäre mithilfe von IKT, oder Art. 199 Strafgesetzbuch, unerlaubte Aufnahmen und Fotografien.[50] **Diskriminierung und Anstiftung zu Hass und Gewalt** gemäß **Artikel 240** können ebenfalls über elektronische Mittel erfolgen.

Erpressung im Sinne von Artikel 223 Strafgesetzbuch erfolgt normalerweise über den Einsatz von Ransomware. Dabei wird in der Regel ein einzelnes System blockiert, indem die dort gespeicherten Daten oder die Programmdateien verschlüsselt werden. Für die Entschlüsselung wird dann eine hohe Geldsumme gefordert (häufig zahlbar in Bitcoins).

Weitere Beispiele:

Rufschädigung durch Beleidigungen oder Anschuldigungen auf Webseiten, Blogs oder über E-Mail-Verteiler. Das elektronische Medium ist insofern relevant, als dass es für die Veröffentlichung der beleidigenden oder verleumdenden Inhalte eingesetzt wird und größeres Potenzial hat, das geschützte Rechtsgut zu verletzen (vgl. Art. 183/1 a Strafgesetzbuch: Beleidigung über Mittel, die deren Verbreitung vereinfachen; und Nr. 3 Strafgesetzbuch: Massenkommunikationsmittel, z. B. soziale Netzwerke).

Rechtsverordnung Nr. 7/2004 vom 7. Januar implementierte Richtlinie 2000/31/EG. Dieses Instrument begründete das Prinzip, dass intermediäre Netzwerkdienstanbieter nicht für potenziell illegale Inhalte auf ihren Plattformen verantwortlich gemacht werden können. Man nimmt Abstand von einer generellen Verpflichtung seitens des intermediären Dienstanbieters, die übertragenen, gespeicherten oder zugänglich gemachten Daten zu überprüfen (Art. 12) und verpflichtet sie stattdessen, umgehend die Strafverfolgungsbe-hörden zu informieren, sollten sie auf potenziell illegale Inhalte auf ihren Plattformen aufmerksam werden (Art. 13 a). Die letzte Änderung erfolgte durch

[50] Cibercrime and *Stalking*, Vânia Costa Ramos, p. 11. https://carlospintodeabreu.com/public/files/cibercrime_stalking.pdf

Gesetzentwurf Nr. 187/XIV/1, der diese Informationspflicht erweitert und hinsichtlich der Entdeckung jeglicher durch den Dienstanbieter verfügbar gemachten, potenziell illegalen Inhalte stärkt, besonders im Hinblick auf Kinderpornografie und Diskriminierung und Anstiftung zu Hass und Gewalt.[51]

Neben der Meldungspflicht gegenüber den Behörden sind intermediäre Dienstanbieter, sofern sie selbst oder durch Dritte auf **offensichtlich** illegale Inhalte aufmerksam werden, auch zu deren Blockierung oder Löschung verpflichtet (vgl. Art. 13 c); Art. Art. 15, Paragraf 3; Art. Art. 16, Paragraf 1; Art. 17). Seit den Änderungen durch Gesetzentwurf Nr. 187/XIV/1 sind Anbieter verpflichtet, Inhalte, die den sexuellen Missbrauch oder die sexuelle Ausbeutung Minderjähriger zeigen, innerhalb von 48 Stunden zu entfernen.[52]

Kommt der Anbieter seiner Melde- und Löschungspflicht nicht nach, wird er entweder zivilrechtlich (Art. 16) oder gemäß in Form einer Ordnungswidrigkeit (Art. 37) gegenüber der Aufsichtsbehörde ANACOM haftbar.

Gesetz 32/2008 vom 17. Juli 2008 über die sog. Vorratsdatenspeicherung (portugiesisch: Lei de Retenção de Dados, LRD) verpflichtete Anbieter elektronischer Kommunikations-dienste zur Speicherung von Kommunikationsdaten für die Untersuchung, Feststellung und Verfolgung schwerer Straftaten durch die zuständigen Behörden. Es setze Richtlinie 2006/24/EG um, die im europäischen Recht nicht länger gültig ist.[53] Allerdings ist das Gesetz im portugiesischen Justizsystem nach wie vor gültig. Die wichtigsten Bestimmungen bezüglich der Speicherung digitaler Beweismittel sind in Artikel 4, Paragraf 3 festgehalten, die die Kriterien für eine schwere Straftat im Sinne dieses Gesetztes festlegen und daher eine Liste der Straftaten enthalten, deren Untersuchung die Verwendung der durch die Dienstanbieter gespeicherten Daten rechtfertigt, und Artikel 6, der im elektronischen Kommunikationssektor **für die Speicherung von Verkehrs- und Ortsdaten einen Zeitraum von einem Jahr** festlegt.

Gesetz 46/2018 vom 13 August schuf die **gesetzlichen Rahmenbedingungen für Sicherheit im Cyberspace** (Regime Jurídico da Segurança do Ciberespaço), und setzte die Richtlinie (EU) 2016/1148 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union um[54]. Damit wurde die CSSC (Conselho Superior de Segurança do Ciberespaço) als Sonderbehörde gegründet, die dem Ministerpräsidenten in Sicherheitsfragen zum Cyberspace berät. Artikel 5 und 6 des Gesetzes definieren die Kompetenzen des CSSC und Artikel 7 die des Nationalen Zentrums für Cybersicherheit (Centro Nacional de Cibersegurança CNCS). Artikel 8 und 9 legen die gesetzlichen Rahmenbedingungen für das National Computer Security Incident Response Team – Equipa de Resposta a Incidentes de Segurança Informática Nacional CERT.PT – sowie dessen Kompetenzen innerhalb des CNSC fest. Das Gesetz legt außerdem ein Mindestmaß an Cybersicherheitsmaßnahmen und eine Meldeverpflichtung für Vorfälle auf allen Regierungsebenen, für alle Behörden, kritischen Infrastrukturdienstleister, Betreiber systemrelevanter Einrichtungen sowie Anbieter digitaler Dienstleistungen an das CNCS, das gegebenenfalls die Pendants in anderen betroffenen Mitgliedsstaaten informiert.

Am 12. Juni 2019 verabschiedete die Regierung **die Entschließung des Ministerrates Nr. 92/2019 und damit die erste Nationale Strategie für Sicherheit im Cyberspace**, die die Sicherheit von

[51] Siehe neuer Artikel 19-A der Rechtsverordnung Nr. 7/2004, der nach Bestätigung des Gesetzentwurfs Nr. 187/XIV hinzugefügt wurde.

[52] Siehe Artikel 19 B der Rechtsverordnung Nr. 7/2004, der nach der Bestätigung von Gesetzentwurf Nr. 187/XIV/1 hinzugefügt wurde und explizit die Entfernung von Inhalten, die sexuellen Missbrauch oder sexuelle Ausbeu-tung von Minderjährigen zeigen, innerhalb von 48 fordert.

[53] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32006L0024&from=PT

[54] Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=PT 187/XIV hinzugefügt wurde.

Netzwerken und Informationssystemen verbessern und allen Bürgern und privaten wie staatlichen Einrichtungen die freie, sichere und effiziente Nutzung des Cyberspace ermöglichen soll. Die Strategie basiert auf drei Prinzipien: Subsidiarität staatlicher Intervention, Komplementarität der Handlung (enge Zusammenarbeit und Koordination verschiedener Handlungsträger) und Proportionalität (bei der Verteilung von Ressourcen und Diensten für den Umgang mit digitalen Bedrohungen).

2.3.2. Rumänien

Das rumänische Rechtssystem verfügt über keine gesonderte Gesetzgebung bezüglich Cyberkriminalität. Daher finden sich die gesetzlichen Bestimmungen für diese Art von Straftat im rumänischen Strafgesetzbuch, und zwar in zwei verschiedenen Teilen.

II. Teil - Verbrechen und Vergehen gegen das Eigentum
Kapitel IV - Betrug durch Computersysteme oder elektronische Zahlungsmittel:

- Computerbetrug (Art. 249) wird definiert als das „Hinterlegen, Verändern oder Löschen von Computerdaten, Beschränken des Zugangs zu solchen Daten, oder in jeglicher anderer Art und Weise die Behinderung des Normalbetriebs eines Computersystems mit dem Ziel, vom verursachten Schaden zu profitieren";
- Durchführung betrügerischer Finanztransaktionen (Art. 250) - „Die Ausführung von Barabhebungen oder Einzahlungen, das Herunterladen elektronischer Zahlungsinstrumente oder der Transfer von Geldmitteln über elektronische Zahlungsmethoden ohne die Zustimmung des Eigentümers und ohne dessen zweifelsfreie Identifikatoren";
- Annahme betrügerischer Finanztransaktionen (Art. 251) - „Die Annahme o. g. Transaktionen im Wissen um deren betrügerische Herkunft";

VII. Teil - Verbrechen und Vergehen gegen die öffentliche Sicherheit
Kapitel VI - Verbrechen und Vergehen gehen die Sicherheit und Integrität von Computersystemen und Daten

- Illegaler Zugriff auf ein Computersystem (Art. 360) unterscheidet zwischen illegalem Zugriff auf ein Computersystem, illegalem Zugriff auf ein Computersystem zum Zweck des Datenerhalts und illegalem Zugriff auf ein Computersystem, welches durch Programme, Geräte oder Abläufe gegen solche Zugriffe geschützt ist. Die drei Arten von Verbrechen bzw. Vergehen ziehen Strafen zunehmender Härte nach sich;
- Illegales Abfangen elektronisch verarbeiteter Daten (Art. 361)
- Veränderung der Integrität von Computer Daten (Art. 362) - „Das illegale Verändern, Löschen, Verschlechtern oder Beschädigen von Computerdaten oder Beschränkung des Zugriffs auf dieselben";
- Störung des Betriebs von Computersystemen (Art. 363) - „erhebliche und unerlaubte Störung des Betriebs von Computersystemen durch Eingabe, Übertragung, Veränderung, Löschung oder Verschlechterung von Computerdaten oder Beschränkung des Zugriffs auf dieselben";
- Unerlaubte Übertragung von Computerdaten (Art. 364)

- Illegale Handlungen mithilfe von Computergeräten oder Software (Art. 365) - „Herstellung, Import, Verteilung, Überlassung oder illegaler Besitz von Geräten, Programmen, Passwörtern oder Zugangscodes, die ganz oder teilweise Zugriff auf Computersysteme zum Zweck der Durchführung von Straftaten gemäß Artikel 360 bis 364 ermöglichen.

VIII. Teil - Verbrechen und Vergehen gegen zwischenmenschliche Beziehungen
Kapitel I - Verbrechen und Vergehen gegen den Frieden und die öffentliche Ordnung

- Kinderpornografie (Art. 374), definiert als das „Produzieren, Besitzen, Erlangen, Aufbewahren, Ausstellen, Bewerben, Verbreiten oder Weitergeben und/oder in jeglicher Art das Bereitstellen pornografischer Inhalte mit Minderjährigen, sowie das Zwingen oder Anstellen Minderjähriger zum Zweck der Teilnahme an den Dreharbeiten pornografischer Inhalte, davon einen Vorteil zu erlangen, oder Minderjährige anderweitig zum Zweck einer pornografischen Darstellung auszubeuten". Das Ansehen kinderpornografischer Inhalte steht ebenso unter Strafe. Die Cyberkriminalitätskomponente bezüglich Kinderpornografie geht klar aus Artikel 374, Abschnitt 2, hervor, der ausdrücklich die Bestrafung für die o. g. Handlungen nennt, unabhängig davon, ob diese mithilfe eines Computersystems oder anderer elektronischer Kommunikationsmittel ausgeführt wurden. Des Weiteren schließt Abschnitt 4 neue Informations- und Kommunikationstechnologien ausdrücklich in die Kommunikationsmittel für pornografische Darstellungen mit ein.

Allein der Versuch der o. g. Handlungen ist in Übereinstimmung mit den Artikeln 252, 366 und 374(5) des rumänischen Strafgesetzbuchs strafbar.

Das Engagement der rumänischen Regierung im Kampf gegen Cyberkriminalität wurde 2011 erneuert, als man dort ein National Computer Security Incident Response Team (Rumänisch:) *Centrul Naţional de Răspuns la Incidente de Securitate Cibernetică* - CERT-RO) gründete, das aus einem unabhängigen und spezialisierten Forschungs- und Entwicklungszentrum im Bereich Cybersicherheit besteht. Rumänien verabschiedete 2013 die Nationa-le Strategie für Cybersicherheit, die auf die Schaffung eines Nationalen Systems für Cyber-sicherheit (Rumänisch: *Sistemul naţional de securitate cibernetică* - SNSC) abzielte, das auf einem allgemeinen Rahmen für bereichsübergreifende Kooperation zwischen Behörden und Institutionen der Industrie oder deren Vertreter basiert.

Im Juli 2020 wurde Gesetz 217/2003 zur Prävention und Kampf gegen häusliche Gewalt um den Aspekt der Gewalt im Internet erweitert, neben den anerkannten Formen häuslicher Gewalt wie verbale, physische, sexuelle, psychologische, wirtschaftliche, geistliche und soziale Gewalt. Gemäß Gesetz 217/2003 ist Gewalt im Internet definiert als „Online-Belästigung, Online-Hassrede, Online-Stalking, Online-Drohungen, nicht einvernehmliche Veröffentlichung von Informationen und intimen Inhalten, illegales Zugreifen oder Abfangen privater Kommunikation und Daten und jegliche andere Form des Missbrauchs von Informations- und Kommunikationstechnologien über Computer, Smartphones oder ähnliche Geräte, die das Telekommunikationsnetzwerk nutzen oder sich mit dem Internet verbinden und Daten übertragen oder sich mit sozialen oder E-Mail-Plattformen verbinden können, um das Opfer zu schikanieren, erniedrigen,

einschüchtern, bedrohen oder zum Schweigen zu bringen."[55] Es darf nicht außer Acht gelassen werden, dass sich diese Bestimmungen auf absichtliche Handlungen oder Unterlassungen beziehen, die jeglicher o. g. Form der Gewalt miteinschließen und „in einem häuslichen oder familiären Umfeld, zwischen Ehepartnern oder Ex-Ehepartnern, zwischen Lebenspartnern oder Ex-Lebenspartnern vorkommen, unabhängig davon, ob der Täter mit dem Opfer zusammenwohnt oder zusammengewohnt hat" (Art. 3).

Zum Zeitpunkt der Erstellung dieses Handbuch diskutierte das rumänische Parlament einen Gesetzesvorschlag, der nichteinvernehmliche Pornografie (sog. „Rachepornografie"[56]) unter Strafe stellen sollte. Dieser war am 21. Oktober 2019 vom Senat angenommen und zur Diskussion an die Abgeordnetenkammer weitergegeben worden. Der Gesetzesvorschlag sieht eine Änderung des Artikels 226 des Strafgesetzbuches vor (der das Strafmaß für Verstöße gegen die Privatsphäre bzw. Persönlichkeitsrechte regelt). Nichteinvernehmliche Pornografie, für diesen Zweck definiert als „das Teilen, Zeigen oder Übertragen intimer Bilder einer Person ohne deren Zustimmung, unabhängig vom dazu verwendeten Mittel", soll als Vergehen in Artikel 226 aufgenommen und mit einem Strafmaß von 3 Monaten bis zu 2 Jahren Gefängnis oder einer Geldstrafe geahndet werden.[57]

2.3.3. Deutschland

Mit dem Inkrafttreten der Lanzarote- und der Budapest-Konvention wurde auch die deutschen Strafgesetze an die aktuellen Entwicklungen im Bereich Internet und Computerkriminalität angepasst. Entsprechend übernahm auch die deutsche Gesetzgebung wichtige EU-Richtlinien über Cyber-Angriffe und den Schutz von Kindern vor sexuellem Missbrauch, Ausbeutung von Minderjährigen und Kinderpornografie. Wichtige Änderungen waren die Kriminalisierung von Cyber-Grooming Minderjähriger und Anpassung der Strafen gemäß der Lanzarote-Konvention.

Das **BKA** (Bundeskriminalamt) ist als **Bundesbehörde** sowohl auf nationaler als auch auf der Ebene internationaler Zusammenarbeit für **Cyberkriminalität** zuständig, besonders im Bereich Kartenbetrug im Internet. Im Kampf gegen Cyberkriminalität arbeitet das BKA direkt mit Behörden wie Interpol und Europol zusammen.

Das Innenministerium entwickelte nationale Strategien für die Bekämpfung von Cyberkriminalität, die Stärkung der Sicherheit von Telekommunikations- und Computersystemen und die Verbesserung des Schutzes von Internetnutzern in Deutschland.[58] Die erste Strategie trat 2011 in Kraft und ihre Ziele sind größtenteils bis heute aktuell. Die schnelle Entwicklung des Phänomens führte dazu, dass diese Ziele 2016 ergänzt und in eine neue Strategie aufgenommen werden mussten, die die Querverbindungen verschiedener Dienste und Akteure berücksichtigt und die Kooperation zwischen Handlungsträgern fördert und beschleunigt und die bereichsübergreifende Natur der Cyberkriminalität berücksichtigt.[59]

Hinsichtlich der gesetzlichen Regelungen im Kampf gegen Cyberkriminalität, angefangen beim Grundgesetz, das explizit das Brief- und Kommunikationsgeheimnis schützt, über die Bestimmungen

[55] Artikel 4 (h) des Gesetzes 217/2003, geändert durch Gesetz 106 vom 3. Juli 2020.

[56] Der Verfasser spricht sich ausdrücklich gegen die Verwendung des Ausdrucks „Rachepornografie" aus, da dieser ein Fehlverhalten des Opfers impliziert und dem Täter das Recht zuschreibt, das Material als eine Art der Bestrafung zu veröffentlichen. Des Weiteren impliziert der Ausdruck „Pornografie", dass das Material für ein größeres Publikum und/oder zur sexuellen Erregung produziert wurde, während viele dieser Vergehen primär auf die Kontrolle und den Missbrauch des Opfers abzielen. Daher ist „nicht-einvernehmliche Verbreitung sexu-eller Inhalte" der präferierte Terminus.

[57] Weitere Informationen über den Gesetzesvorschlag bezüglich nichteinvernehmlicher Pornografie erhalten Sie unter https://www.senat.ro/legis/lista.aspx?nr_cls=L512&an_cls=2019.

[58] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy-for-germany

[59] https://www.bmi.bund.de/cybersicherheitsstrategie/

des Strafgesetzbuchs bis hin zu eigenen Gesetzen wie dem **Telekommunikationsgesetz (TKG)**, dem **Telemediengesetz (TMG)**, dem **IT-Sicherheitsgesetz** und dem **Netzwerkdurchsetzungsgesetz (NetzDG)**, ist das deutsche Rechtssystem gut an die Dynamic und Überregionalität von Cyberkriminalität angepasst und sieht auch die enge Zusammenarbeit mit privaten Institutionen auf nationaler Ebene vor.

Das gleiche gilt für das **Jugendschutzgesetz (JuSchG)**, das Kindern und Jugendlichen verschiedener Altersgruppen den Zugang zu gesundheitsgefährdenden Produkten, Kinofilmen, Medien auf Datenträgern und einigen öffentlichen Orten verbietet oder beschränkt, um sie zu schützen und um ihre Rechte zu stärken. Derzeit wird eine Änderung des Gesetzes diskutiert, die einen stärkeren Fokus auf die Verhinderung von Cyber-Grooming und Cybermobbing vorsieht.

Artikel 10 des Grundgesetzes schützt das Briefgeheimnis sowie das Post- und Fernmeldegeheimnis.

Das **Strafgesetzbuch (StGB)** definiert die mit Cyberkriminalität in Verbindung stehenden Vergehen. Es findet keine Unterscheidung zwischen allgemeinem Strafgesetz und Gesetzen bezüglich Cyberkriminalität statt, wie es im portugiesischen Rechtssystem der Fall ist.

Das StGB sieht drei Arten cyberkrimineller Vergehen vor:

1. Taten, in deren Rahmen **Computersysteme oder Daten auf illegale Weise verwendet werden**, besonders im Hinblick auf Cyber-Angriffe:

Tat	Art	Artikel in der Budapest-Konvention
Sich oder einem anderen unbefugt Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschaffen.	Halböffentlich	2
Sich oder einem anderen unbefugt und unter Anwendung von technischen Mitteln nicht für ihn bestimmte Daten aus einer nichtöffentlichen Datenübermittlung oder aus der elektromagnetischen Abstrahlung einer Datenverarbeitungsanlage verschaffen. Kann in Bezug auf weitere Taten *strafverschärfend* wirken.		3
Das Vorbereiten der in § 202a und 202b beschriebenen Taten, z. B. Zugangscodes, die den Zugang zu Daten ermöglichen oder Computerprogramme, deren Zweck die Begehung einer solchen Tat ist, herzustellen, sich oder einem anderen zu verschaffen, zu verkaufen, einem anderen zu überlassen, zu verbreiten oder sonst zugänglich zu machen.		6
Daten, die nicht allgemein zugänglich sind und die **ein anderer durch eine rechtswidrige Tat erlangt hat**, sich oder einem anderen zu verschaffen, einem anderen zu überlassen, zu verbreiten oder sonst zugänglich zu		

	machen, um sich oder einen Dritten zu bereichern oder einen anderen zu schädigen. Ausnahme: Handlungen, die ausschließlich der Erfüllung rechtmäßiger dienstlicher oder beruflicher Pflichten dienen, z. B. von Amtsträger im Rahmen eines Verfahrens.	
	Daten löschen, unterdrücken, unbrauchbar machen oder verändern.	4
	(1) Eine Datenverarbeitung, die für einen anderen von wesentlicher Bedeutung ist, dadurch erheblich zu stören, dass er eine Tat nach § 303a Abs. 1 begeht; oder Daten in der Absicht, einem anderen Nachteil zuzufügen, eingibt oder übermittelt; oder eine Datenverarbeitungsanlage oder einen Datenträger zerstört, beschädigt, unbrauchbar macht, beseitigt oder verändert. (5) Für die Vorbereitung einer Straftat gilt § 202c entsprechend.	5
	Zur Täuschung im Rechtsverkehr beweiserhebliche Daten so speichern oder verändern, dass bei ihrer Wahrnehmung eine unechte oder verfälschte Urkunde vorliegen würde, oder derart gespeicherte oder veränderte Daten gebrauchen.	7
	Der Täuschung im Rechtsverkehr steht die fälschliche Beeinflussung einer Datenverarbeitung im Rechtsverkehr gleich.	7

2. Taten, deren **Begehung den Einsatz elektronischer Mittel als Werkzeug erfordert**:

Artikel und Überschrift	Tat	Art	Artikel in der Budapest-Konvention
§ 206 – **Verletzung des Post- oder Fernmeldegeheimnisses**	(1) Unbefugt einer anderen Person eine Mitteilung über Tatsachen machen, die dem Post- oder Fernmeldegeheimnis unterliegen und die einem als Inhaber oder Beschäftigtem eines Unternehmens bekanntgeworden sind, das geschäftsmäßig Post- oder Telekommunikationsdienste erbringt. Dem Postgeheimnis unterliegen die näheren Umstände des Postverkehrs bestimmter Personen sowie der Inhalt von Postsendungen. Dem **Fernmeldegeheimnis unterliegen der Inhalt der Telekommunikation und ihre näheren Umstände**, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war. Das Fernmeldegeheimnis erstreckt sich auch auf die näheren Umstände **erfolgloser Verbindungsversuche**.		
§ 263a – **Computerbetrug**	(1) In der Absicht, sich oder einem Dritten einen rechtswidrigen Vermögensvorteil zu verschaffen, das Vermögen eines anderen dadurch zu beschädigen, dass das Ergebnis eines Datenverarbeitungsvorgangs durch unrichtige Gestaltung des Programms, durch Verwendung unrichtiger oder unvollständiger Daten, durch unbefugte Verwendung von Daten oder sonst durch unbefugte Einwirkung auf den Ablauf beeinflusst wird. (3) Vorbereitende Handlungen wie Computerprogramme, deren Zweck die		8

	Begehung einer solchen Tat ist, herzustellen, sich oder einem anderen zu verschaffen, feilzuhalten, zu verwahren oder einem anderen zu überlassen.
§ 265a – **Erschleichen von Leistungen**	Die Leistung eines Automaten oder eines öffentlichen Zwecken dienenden Telekommunikationsnetzes, die Beförderung durch ein Verkehrsmittel oder den Zutritt zu einer Veranstaltung oder einer Einrichtung in der Absicht zu erschleichen, das Entgelt nicht zu entrichten.

3. Taten, die **mithilfe elektronischer Mittel als Werkzeug** begangen werden können, aber nicht müssen.

In diesem Fall muss berücksichtigt werden, **dass § 11(3)** Inhalte auf Ton- oder Bildträgern, in Datenspeichern, Abbildungen oder anderen Verkörperungen im Sinne der Vorschriften, die auf diesen Absatz verweisen, gleichbehandelt werden müssen. Die folgenden Straftatbestände beinhalten Taten, die mithilfe elektronischer Mittel begangen werden:

Artikel und Überschrift	Tat	Art
§ 86 – **Verbreiten von Propagandamitteln verfassungswidriger Organisationen**	Propagandamittel – gemäß § 11 (3) – die sich nach ihrem Inhalt gegen die verfassungsmäßige Ordnung oder gegen den Gedanken der Völkerverständigung richten, in Deutschland zu verbreiten, der Öffentlichkeit zugänglich zu machen oder zur Verbreitung im Inland oder Ausland herzustellen, vorrätig zu halten, ein- oder auszuführen.	
§ 88 – **Verfassungsfeindliche Sabotage**	(1) Wer absichtlich den Betrieb von (2) Telekommunikationsanlagen, die öffentlichen Zwecken dienen, ... stört.	
§ 91 – **Anleitung zur Begehung einer schweren staatsgefährdenden Gewalttat**	Einen Inhalt gemäß § 11 Absatz 3, der geeignet ist, als Anleitung zu einer schweren staatsgefährdenden Gewalttat (§ 89a) zu dienen, anzupreisen oder einer anderen Person zugänglich zu machen, wenn die Umstände seiner Verbreitung geeignet sind, die Bereitschaft anderer zu fördern oder zu wecken, eine schwere staatsgefährdende Gewalttat zu begehen, und/oder (2) sich für den in (1) beschriebenen Zweck einen Inhalt nach 11 (3) zu verschaffen.	
§ 130 – **Volksverhetzung**	(2) Zu Hass, Gewalt oder Willkürmaßnahmen gegen eine Gruppe, gegen Teile der Bevölkerung oder gegen einen Einzelnen wegen seiner Zugehörigkeit zu einer Gruppe oder zu einem Teil der Bevölkerung über in § 11 (3) bezeichnete Mittel aufzustacheln und diese mittels Rundfunk oder Telemedien der Öffentlichkeit zugänglich zu machen. (5) Eine unter der Herrschaft des Nationalsozialismus begangene Handlung öffentlich zu billigen, leugnen oder verharmlosen oder den öffentlichen Frieden in einer die Würde der Opfer verletzenden Weise dadurch zu stören, dass die nationalsozialistische Gewalt- und Willkürherrschaft gebilligt, verherrlicht oder gerechtfertigt wird, ist ebenso strafbar, wenn dies über Telekommunikationskanäle erfolgt.	
§ 131 – **Gewaltdarstellung**	(1) Einen Inhalt (§ 11 Absatz 3), der grausame oder sonst unmenschliche Gewalttätigkeiten gegen Menschen oder menschenähnliche Wesen in einer Art schildert, die eine Verherrlichung oder Verharmlosung solcher Gewalttätigkeiten ausdrückt, zu verbreiten oder der über Rundfunk oder Telemedien der Öffentlichkeit zugänglich zu machen oder diese Inhalte herzustellen, zu beziehen, zu liefern, vorrätig zu halten, anzubieten, zu bewerben oder es zu unternehmen, diese ein- oder auszuführen.	

§ 201a – **Verletzung des höchstpersönlichen Lebensbereichs und von Persönlichkeitsrechten durch Bildaufnahmen**	(1) Unbefugt eine Bildaufnahme von einer anderen Person, die sich in einer Wohnung oder einem gegen Einblick besonders geschützten Raum befindet, herzustellen oder zu übertragen und dadurch den höchstpersönlichen Lebensbereich der abgebildeten Person zu verletzen. (3) Eine Bildaufnahme, die die Nacktheit einer anderen Person unter 18 Jahren zum Gegenstand hat, herzustellen oder anzubieten, um sie einer dritten Person gegen Entgelt zu verschaffen, oder sich oder einer dritten Person gegen Entgelt zu verschaffen.
§ 238 – **Nachstellung**	Einer anderen Person in einer Weise unbefugt nachstellen, die geeignet ist, deren Lebensgestaltung schwerwiegend zu beeinträchtigen, indem man beharrlich: 1. die räumliche Nähe dieser Person aufsucht, 2. unter Verwendung von Telekommunikationsmitteln Kontakt zu dieser Person herzustellen versucht, 3. unter missbräuchlicher Verwendung von personenbezogenen Daten dieser Person (a) Bestellungen von Waren oder Dienstleistungen für sie aufgibt oder (b) Dritte veranlasst, Kontakt mit ihr aufzunehmen, oder 4. diese Person mit der Verletzung von Leben, körperlicher Unversehrtheit, Gesundheit oder Freiheit ihrer selbst, eines ihrer Angehörigen oder einer anderen ihr nahestehenden Person bedroht.

Verbrechen gegen Minderjährige sind im Folgenden separat aufgeführt, auch wenn sie zu Kategorie (3) gehören:

Artikel und Überschrift	Tat	Art	Artikel in der Budapest-Konvention
§ 176 – **Sexueller Missbrauch von Kindern**	(1) Sexuelle Handlungen an Personen unter 14 Jahren vorzunehmen oder an sich von dem Kind vornehmen zu lassen; (2) Ein Kind dazu zu bestimmen, sexuelle Handlungen an einem Dritten vorzunehmen oder vornehmen zu lassen; (4) Sexuelle Handlungen vor einem Kind vorzunehmen oder auf ein Kind mittels eines Inhalts (§ 11 Absatz 3) oder **Informations- und Kommunikationstechnologien** einwirkt, um das Kind zu sexuellen Handlungen zu bringen, die es an oder vor dem Täter oder einer dritten Person vornehmen oder von dem Täter oder einer dritten Person an sich vornehmen lassen soll, oder auf ein Kind mittels eines pornografischen Inhalts oder durch entsprechende Reden einwirkt. (5) Ein Kind für eine Tat nach den Absätzen (1) bis (4) anzubieten.		9
§ 176a – **Schwerer sexueller Missbrauch von Kindern**	(3) In den Fällen des § 176 als Täter oder anderer Beteiligter in der Absicht zu handeln, die Tat zum Gegenstand eines pornografischen Inhalts (§ 11 Absatz (3)) zu machen, der nach § 184b verbreitet werden soll.		
§ 184b – **Verbreitung, Erwerb und Besitz kinderpornografischer Inhalte (unter 14 Jahren)**	Einen kinderpornografischen Inhalt zu verbreiten oder der Öffentlichkeit zugänglich zu machen, oder einen kinderpornografischen Inhalt herzustellen, zu beziehen, zu liefern, vorrätig zu halten, anzubieten, zu bewerben oder es zu unternehmen, diesen ein- oder auszuführen;		

	kinderpornografisch ist ein pornografischer Inhalt [§ 11 Absatz 3], wenn er zum Gegenstand hat: sexuelle Handlungen von, an oder vor einer Person unter vierzehn Jahren [Kind], die Wiedergabe eines ganz oder teilweise unbekleideten Kindes in aufreizend geschlechtsbetonter Körperhaltung oder die sexuell aufreizende Wiedergabe der unbekleideten Genitalien oder des unbekleideten Gesäßes eines Kindes. [5] Gilt nicht für Handlungen, die ausschließlich der rechtmäßigen Erfüllung staatlicher Aufgaben dienen [z. B. strafrechtliche Ermittlungsverfahren]
§ 184c – **Verbreitung, Erwerb und Besitz jugendpornografischer Inhalte**	Einen jugendpornografischen Inhalt gemäß § 11[3] zu verbreiten oder der Öffentlichkeit zugänglich zu machen, einer anderen Person zugänglich zu machen, oder jungendpornografische Inhalte [zwischen 14 - 18 Jahren] herzustellen, zu beziehen, zu liefern, vorrätig zu halten, anzubieten, zu bewerben oder es zu unternehmen, diesen ein- oder auszuführen.
§ 184d – **Zugänglichmachen pornografischer Inhalte mittels Rundfunk oder Telemedien**	[1] Nach den §§ 184 bis 184c wird auch bestraft, wer einen pornografischen Inhalt mittels Rundfunk oder Telemedien einer anderen Person oder der Öffentlichkeit zugänglich macht. [In den Fällen des § 184 [1] – Verbreitung pornografischer Inhalte – bei einer Verbreitung mittels Telemedien nicht anzuwenden, wenn sichergestellt ist, dass der pornografische Inhalt Personen unter 18 Jahren nicht zeigt und ihnen nicht zugänglich ist]; [2] Nach §§ 184b [3] und 184c [3] wird auch bestraft, wer es unternimmt, einen kinderpornografischen Inhalt mittels Telemedien abzurufen.

Der Versuch ist strafbar gemäß 263a(2) in Verbindung mit § 263(2), § 269(2), § 263a(3), § 303a, § 303b (vgl. § 303a(2) und 303b(3)). Beim Missbrauch von Kindern ist der Versuch ebenso strafbar § 176(6). Ausnahme: § 176 (4) 3 und 4 und § 176 (5). Die Vorbereitung der Straftat in den folgenden Fällen strafbar: § 202c, § 202a, § 202b, § 303a(1)(2) und § 303b (1)(5). Beihilfe ist gemäß §§ 26 und 27 StGB ebenfalls strafbar.

Juristische Personen unterliegen nicht dem Strafrecht, können aber gemäß §§ 30, 130 *Ordnungswidrigkeitengesetz* (OWiG) belangt werden. Ihre gesetzlichen Vertreter können gemäß § 14 StGB belangt werden.

Zusätzlich zu den o. g. Straftaten, beinhaltet das deutsche Recht weitere Vorschriften bezüglich Verbrechen und Ordnungswidrigkeiten in Verbindung mit elektronischer Kommunikation und Datenschutz, die wir kurz zusammenfassen.

Das **Telekommunikationsgesetz (TKG)** vom 22.06.2004 beinhaltet eine Reihe von Verpflichtungen für den Betrieb bei privaten Anbietern von Telekommunikationsdienstleistungen. Dieses Gesetz ist besonders im Hinblick auf die Speicherung digitaler Beweismittel von größter Wichtigkeit. Es verpflichtet zur Meldung von Handlungen, die einen Bruch des Telekommunikationsgeheimnisses darstellen könnten, und zur Speicherung bestimmter Daten, damit im Fall einer schweren Straftat strafrechtlich ermittelt werden kann.

§ 88 Fernmeldegeheimnis und **§ 89 Abhörverbot, Geheimhaltungspflicht der Betreiber von Empfangsanlagen** schützen die Integrität und Vertraulichkeit der Telekommunikation und umfassen sowohl deren Inhalte als auch die genauen Umstände, z. B. wer an einem Telekommunikationsprozess teilnimmt oder teilnahm, und erstreckt sich sogar auf nicht erfolgreiche Verbindungsversuche. Die Parteien dürfen keinerlei Informationen über den Telekommunikationsprozess einholen, die über das hinausgehen, was für ihre Aktivitäten zwingend erforderlich ist. Dieses Wissen darf ausschließlich im Rahmen der geltenden Gesetze oder anderen Rechtsvorschriften anderweitig verwendet werden. In diesem Fall muss darauf hingewiesen werden, dass die Meldepflicht gemäß § 138 StGB – über Straftaten, von denen eine Partei Kenntnis erlangt – gegenüber dem Kommunikationsgeheimnis Priorität hat.

§90 verbietet den **Missbrauch von Sende- oder sonstigen Telekommunikationsanlagen**: Es ist verboten, Sendeanlagen oder sonstige Telekommunikationsanlagen zu besitzen, herzustellen, zu vertreiben, einzuführen oder sonst in den Geltungsbereich dieses Gesetzes zu verbringen, die in besonderer Weise geeignet und dazu bestimmt sind, das nicht öffentlich gesprochene Wort eines anderen von diesem unbemerkt abzuhören oder das Bild eines anderen von diesem unbemerkt aufzunehmen.

§ 96 und § 98 regeln die Bedingungen, unter denen Dienstanbieter **Verkehrs- und Standortdaten** erheben dürfen. Ausschließlich Daten, die für die Aktivität unverzichtbar sind, dürfen gespeichert werden. Solche Daten dürfen nur im erforderlichen Ausmaß und für die in diesem Gesetz genannten Zwecke oder in Übereinstimmung mit anderen Rechtsvorschriften verwendet werden. In jedem anderen Fall müssen sie unverzüglich gelöscht werden.

§ 109 verpflichtet Dienstanbieter zur Einrichtung **technischer Schutzmaßnahmen** zum Schutz des Fernmeldegeheimnisses und gegen die Verletzung des Schutzes personenbezogener Daten und dazu, angemessene technische Vorkehrungen und sonstige Maßnahmen zu treffen, um Nutzer vor Störungen durch äußere Angriffe zu schützen. Insbesondere sind Maßnahmen zu treffen, um Telekommunikations- und Datenverarbeitungssysteme gegen unerlaubte Zugriffe zu sichern und Auswirkungen von Sicherheitsverletzungen für Nutzer oder für zusammengeschaltete Netze so gering wie möglich zu halten. (5) Betreiber müssen der Bundesnetzagentur und dem Bundesamt für Sicherheit in der Informationstechnik unverzüglich Beeinträchtigungen von Telekommunikationsnetzen und -diensten mitzuteilen, die zu beträchtlichen Sicherheitsverletzungen führen können. **§ 109a** über die **Daten- und Informationssicherheit** verpflichtet Betreiber im Fall einer Verletzung des Schutzes personenbezogener Daten unverzüglich die Bundesnetzagentur und den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit von der Verletzung sowie die betroffenen Personen zu benachrichtigen.

§ 113b verpflichtet zur **Speicherung von Verkehrsdaten**: 10 Wochen für Verkehrsdaten und 4 Wochen für Standortdaten. Der Inhalt ist von dieser Vorschrift ausgeschlossen. Der Betreiber hat die gespeicherten Daten unverzüglich, spätestens jedoch binnen einer Woche nach Ablauf der Speicherfristen, irreversibel zu löschen oder die irreversible Löschung sicherzustellen, z. B. Recht auf Vergessenwerden.

§ 113c legt die **Bedingungen der Verwendung** der nach **§ 113b gespeicherten Daten** fest; Sie dürfen an eine Strafverfolgungsbehörde übermittelt werden, soweit diese die Übermittlung unter Berufung auf eine gesetzliche Bestimmung, die ihr eine Erhebung der Daten zur Verfolgung besonders schwerer Straftaten erlaubt, verlangt.

Zu Sicherheit verpflichtet **§ 113d Betreiber zur Gewährleistung der Sicherheit der Daten** auf Grundlage der Verpflichtung gemäß § 113b (1). Gespeicherten Daten durch technische und organisatorische Maßnahmen nach dem Stand der Technik gegen unbefugte Kenntnisnahme und Verwendung geschützt werden, u. a. durch die Verwendung von Verschlüsselungsverfahren.

Die Bundesnetzagentur kann **die Einhaltung der Vorschriften** dieses Gesetzes sicherstellen (**§ 115**). Der Betreiber ist verpflichtet, der Bundesnetzagentur auf Anforderung die erforderlichen Auskünfte zu erteilen. Die Bundesnetzagentur kann dem Betreiber regelmäßige Strafzahlungen auferlegen.

Das Telemediengesetz (TMG) vom 26.02.2007 gilt für alle elektronischen Informations- und Kommunikationsdienste, soweit sie nicht Telekommunikationsdienste sind. Diensteanbieter haben, soweit dies technisch möglich und wirtschaftlich zumutbar ist, im Rahmen ihrer jeweiligen Verantwortlichkeit für geschäftsmäßig angebotene Telemedien durch technische und organisatorische Vorkehrungen sicherzustellen, dass kein unerlaubter Zugriff auf die für ihre Telemedienangebote genutzten technischen Einrichtungen möglich ist (**§ 13(7)**). Andererseits gibt es die **Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten (§ 15d)**.

Das IT-Sicherheitsgesetz vom 25. Juli 2015 regelt die Zuständigkeit der Staatsanwaltschaft für die Untersuchung und Verfolgung von Straftaten gemäß 202a, 202b, 202c, 263a, 303a und 303b StGB.

Es stärkt die Sicherheit von Computer- und IT-Systemen und ist Bestandteil der 2011 verabschiedeten Cybersicherheitsstrategie. Es legt Verpflichtungen für ein Mindestmaß an Computersicherheit für Telekommunikationsunternehmen, Anbieter digitaler Dienste und Betreiber kritischer Infrastruktur fest, z. B. verlangt es die Einrichtung eines IT-Sicherheitsverwaltungssystems, die Meldung von Attacken auf das System an das Bundesamt für Sicherheit in der Informationstechnik (BSI) und Verbraucher und die Speicherung von Informationen, die für eine Beurteilung des Sicherheitsrisikos von Informationstechnologie notwendig sind, in Form von Berichten über die aufgetretenen Angriffe, eingesetzte Abläufe und unmittelbare Risiken, damit diese an Bundesbehörden gemeldet werden können (§ 4).

Das IT-Sicherheitsgesetz 2.0, ein Vorschlag zur Änderung des Gesetzes, wurde bei Fertigstellung dieses Berichts noch diskutiert.[60] Der neue Gesetzesvorschlag basiert auf einer Änderung der Strategie im Kampf gegen Cyberkriminalität, der nicht länger defensiv, sondern offensiv über verschiedene IT-Taktiken geführt werden sollte.[61] Der Vorschlag enthält auch verschärfte Strafen für Cyber-Verbrechen nach §§ 202a, 202b, 202c, 202d, 303a und 303b StGB. Außerdem werden §§ 202e und 202f nach § 202d StGB eingefügt:

[60] https://www.whitecase.com/publications/article/germanys-draft-bill-it-security-20-extended-bsi-authorities-stricter-penalties

[61] https://netzpolitik.org/2019/it-sicherheitsgesetz-2-0-wir-veroeffentlichen-den-entwurf-der-das-bsi-zur-hackerbehoerde-machen-soll/#2019-03-27_BMI_Referentenentwurf_IT-Sicherheitsgesetz-2 and https://netzpolitik.org/2015/geheime-kommunikation-bsi-programmierte-und-arbeitete-aktiv-am-staatstrojaner-streitet-aber-zusammenarbeit-ab/

- § 200e - Unbefugte Nutzung informationstechnischer Systeme;
- § 202f - Besonders schwerer Fall einer Straftat gegen die Vertraulichkeit oder Integrität informationstechnischer Systeme.

Das ***Netzwerkdurchsetzungsgesetz*** **(NetzDG)** vom 1.09.2017 wird umgangssprachlich auch als Facebook-Gesetz bezeichnet und führte bußgeldbewehrte Compliance-Regeln für Anbieter sozialer Netzwerke betreffend den Umgang mit Nutzer-Beschwerden über Hasskriminalität und andere strafbare Inhalte im Netz sowie eine vierteljährliche Berichtspflicht der Anbieter ein. Außerdem eröffnet es Opfern von Persönlichkeitsverletzungen im Inter-net einen Anspruch auf Auskunft über Bestandsdaten des Verletzers aufgrund gerichtlicher Anordnung.[62]

§1 (3) definiert illegale Inhalte,[63] einschließlich Diskriminierung, Anstiftung zur Hassrede und rechtes Gedankengut. § 2 verpflichtet zur regelmäßigen Berichterstattung über den Umgang mit Beschwerden über illegale Inhalte auf der Plattform. Dieser Bericht muss öffentlich zugänglich sein. Das Bundesamt für Justiz (BfJ) ist für diese Berichte zuständig, vgl. § 4 (4).

§ 3(2) 2 **verpflichtet den Betreiber, den Zugang zu offensichtlich illegalen Inhalten innerhalb von 24 Stunden nach Erhalt der Beschwerde zu blockieren oder zu löschen**, sofern dies nicht mit Justizbehörden anders vereinbart ist. Andere illegale Inhalte müssen unverzüglich, spätestens aber sieben Tage nach Erhalt der Beschwerde gelöscht oder der Zugang zu ihnen gesperrt werden, vgl. § 3 (2) 3. Bei einer Löschung ist der Anbieter verpflichtet, die Inhalte zu Beweiszwecken zu speichern. Zu diesem Zweck speichert der Anbieter die Inhalte für die Dauer von zehn Wochen innerhalb des Geltungsbereichs der Richtlinien 2000/31/EG und 2010/13/EU, vgl. § 3 (3).

Die Nichteinhaltung dieser Vorschriften ist strafbar.

Die gesonderten verfahrensrechtlichen Verpflichtungen gemäß Artikel 16 und 17 des Übereinkommens über Computerkriminalität sind nicht explizit in die **Strafprozessordnung (StPO)** aufgenommen worden. Allerdings erfolgt die Beschlagnahmung von Computerdaten, einschließlich der Anfragen zur Offenlegung von Daten gemäß § 94 und § 98 StPO, die die allgemeine Sicherstellung und Beschlagnahme von Gegenständen zu Beweiszwecken regeln.

Artikel 18 des Übereinkommens über Computerkriminalität als solches ist nicht Bestandteil der StPO. Die Anfrage durch Behörden über die Offenlegung von/Information über Computerdaten wird durch § 95 StPO geregelt, der jeden dazu verpflichtet, relevante bewegliche Sachen herauszugeben, die als Beweismittel für die Untersuchung von Bedeutung sein könnten.

Die Erhebung von Verkehrsdaten, die in Artikel 20 des Übereinkommens über Computerkriminalität gefordert wird, ist in § 100g StPO festgelegt. Dieser Paragraf legt außerdem fest, welche schweren Straftaten die Erhebung solcher Daten durch Dienstanbieter rechtfertigen (vgl. § 113b TKG). **§** 100g (2) klärt außerdem die Bedingungen, unter denen ein Gericht die Überlassung von Verkehrsdaten

[62] https://www.europol.europa.eu/content/expert-international-cyber-crime-taskforce-launched-tackle-online-crime Participants: Austria, Canada, Germany, France, Italy, the Netherlands, Spain, UK and USA. Australia and Colombia have committed to the initiative.

[63] https://www.cert-verbund.de/

und Informationen durch Dienstanbieter an-ordnen kann, nämlich wenn bestimmte Tatsachen den Verdacht begründen, dass jemand eine der aufgelisteten schweren Straftaten begangen hat oder zu begehen beabsichtigt.

Die in Artikel 21 des Übereinkommens über Computerkriminalität genannte Überwachung von Telekommunikation oder Erhebung von Echtzeit-Daten wird in § 100a und § 100b geregelt. Sie unterliegt der behördlichen Autorisierungspflicht auf Anordnung der Staatsanwaltschaft. Allgemein ist die Datenerhebung durch Online-Suche und Spyware zum Zweck strafrechtlicher Verfolgung ausschließlich in den in § 100b beschriebenen Fällen erlaubt.

§ 110 (3) – Die Durchsicht eines elektronischen Speichermediums darf auch auf hiervon räumlich getrennte Speichermedien, soweit auf sie von dem Speichermedium aus zugegriffen werden kann, erstreckt werden. Beispiel: externe Festplatten.

§ 100j StPO stellt allgemeine Regelungen hinsichtlich der Verlangung nach Auskunft durch Behörden bei Dienstanbietern bereit, die in weiteren Gesetzen genauer festgelegt sind; z. B. § 113 TKG.

Die Informationen und Daten müssen gemäß § 96(1), § 113a und 113b TKG (Telekommunikationsgesetz) zur Verfügung gestellt werden.

Hinsichtlich **internationaler Kooperation** ist Deutschland in zahlreiche europäische und internationale bilaterale Projekte im Bereich Cybersicherheit involviert:

- Agentur der Europäischen Union für Cybersicherheit (ENISA);
- Das AGIS-Programm der Europäischen Kommission, das ein europäisches Netzwerk zum Austausch von Informationen und bewährten Strategien für Justizbehörden, Anwälte und Vertreter von Opferhilfsorganisationen aus Mitgliedsstaaten und anderen Staaten, die sich bewerben, etablieren soll;
- Die Interpol European Working Party on IT Crime (EWPITC), eine Plattform zum Informationsaustausch und für den Kampf gegen IT-Kriminalität.

Die **Internationale Rechtshilfe in Strafsachen (IRG)** legt Abläufe und Bedingungen für internationale Rechtshilfe fest. Die Artikel 29 - 31 des Übereinkommens über Computerkriminalität über die gegenseitige Unterstützung von Ländern sind Bestandteil dieses Gesetzes.

Hinsichtlich der Zusammenarbeit mit dem Cyberkriminalitätszentrum von Europol ist Deutschland Teil der Joint Cybercrime Action Taskforce (J-CAT).[64]

Die Kontaktstelle, die gemäß Artikel 35 der Budapest-Konvention an sieben Wochentagen 24 Stunden täglich zur Verfügung steht, wurde zusammen mit der Kontaktstelle für Interpol und die G8 beim BKA in Wiesbaden eingerichtet.

[64] https://www.europol.europa.eu/content/expert-international-cybercrime-taskforce-launched-tackle-online-crime Teilnehmer: Österreich, Kanada, Deutschland, Frankreich, Italien, Niederlande, Spanien, das Vereinigte Königreich und die Vereinigten Staaten. Australien und Kolumbien haben sich der Initiative verpflichtet.

Des Weiteren gibt es in Deutschland einige **Partnerschaften zwischen öffentlich und privaten Einrichtungen** zum **Kampf gegen Cyberkriminalität, nämlich**:

- Allianz für Cybersicherheit: fördert den Austausch von Informationen und Erfahrungen unter den wichtigsten deutschen Handlungsträgern im Bereich Cybersicherheit. Die Plattform soll über die Risiken im Cyberspace aufklären und Wissensaustausch fördern. Eine gemeinsame Initiative des Bundesamts für Sicherheit in der Informationstechnik (BSI) und des Bundesverbands Informationswirtschaft, Telekommunikation und neue Medien (Bitkom);
- CERT-Netzwerk – das CERT-Netzwerk ist ein Zusammenschluss der IT-Notfallteams.[65]

Abschließende Hinweise:

- Der bloße Besitz von Schadsoftware ist kein Straftatbestand. Die nationalen Gesetze stellen dies lediglich unter Strafe, wenn eine Person die Schadsoftware für kriminelle Zwecke einsetzt.
- Einige Fachleute fordern, dass in der StPO rechtliche Rahmenbedingungen für den Einsatz von Datenzugriffs-Tools wie bei Hackerangriffen geschaffen werden, unter Berücksichtigung der Tatsache, dass die Sicherheitskräfte stets einen Schritt hinter den Tätern zurückliegen.
- Allgemein scheint das deutsche Gesetz mit den europäischen Rechtstexten übereinzustimmen.
- Trotzdem wurden die Artikel 4 und 5 der Richtlinie 2019/713/EU nicht direkt umgesetzt, da zwei weitere Straftatbestände (§§ 263a StGB Computerbetrug und 269 StGB Fälschung beweiserheblicher Daten) für die Abdeckung von Straftaten in Verbindung der Verwendung von unbaren Zahlungsinstrumenten zu Betrugszwecken herangezogen werden müssen. § 152b StGB stellt die Fälschung von Zahlungskarten unter Strafe, beinhaltet aber keinen Verweis auf den Einsatz elektronischer Mittel oder IT-Systemen.

[65] https://www.cert-verbund.de/

3. KRIMINOLOGISCHE UND VIKTIMOLOGISCHE ANSÄTZE ZUM VERSTÄNDNIS VON CYBERKRIMINALITÄT

3.1. Anwendung kriminologischer Theorien auf Cyberkriminalität

In diesem Kapitel des Handbuchs behandeln wir kurz verschiedene Kriminalitätstheorien und ihre Anwendung auf Cyberkriminalität, um ein möglichst umfassendes Bild des Phänomens der Cyberkriminalität zeichnen zu können.

Die Grundlage für eine solche Analyse ist die Annahme, dass bestehendes Wissen über *herkömmliche Kriminalität* auch auf Cyberkriminalität angewendet werden kann, ausgehend davon, dass sich Cyberkriminalität nicht substanziell von *herkömmlicher Kriminalität* unterscheidet. So werden kriminologische Theorien, die im Zusammenhang mit *herkömmlicher Kriminalität* entwickelt wurde, wertvolle Werkzeuge für die Erklärung von Cyber kriminalität (Wall, 2005, Yar, 2005b *cit in* Bossler & Burruss, 2012).

Es ist auf keinen Fall möglich kriminelle Phänomene und Cyberkriminalität im speziellen durch den Fokus einer einzigen kriminologischen Theorie oder eines solchen Ansatzes zu betrachten. Daher ist es sehr wichtig, stets die Komplexität des Phänomens im Auge zu behalten und bei der Suche nach einem umfassenderen Verständnis von Cyberkriminalität und Cyber-Viktimisierung eine Verflechtung dieser (und anderer) Perspektiven in Betracht zu ziehen (Yar & Steinmetz, 2019).

3.1.1. Individuelle Perspektiven

Dieser Ansatz geht davon aus, dass Individuen mit niedriger Selbstkontrolle wahrscheinli-cher illegale Handlungen verüben. (Gottredson & Hirschi, 1990 *cit in* Maimon & Louderback, 2019).

In dieser Hinsicht argumentieren Gottfredson and Hirschi (1990 *cit in* Higgins, Ricketts & Wolfe, 2014), dass Menschen mit **niedriger Selbstkontrolle** weniger in der Lage sind, einer Versuchung zu widerstehen, wenn sie mit einer Gelegenheit, eine Straftat zu verüben, konfrontiert sind. Die hervorstechendsten Charaktereigenschaften dieses Personentyps, nämlich Impulsivität und mangelnde Sensibilität, lassen sie die Konsequenzen ihrer Hand-lungen unterschätzen. (Gottfredson & Hirschi, 1990 *cit in* idem). In diesem Sinne erscheinen Straftaten attraktiv, da sie sofortigen Profit versprechen, wenn man die langfristigen Folgen sowohl auf individueller Ebene als auch für andere außer Acht lässt.

Wendet man diesen Erklärungsansatz *herkömmlicher* Kriminalität auf die Cyberkriminalität an, scheinen die *individuellen Charakteristika des Cyberkriminellen* und *Cyberkriminalität* nicht so linear. Die Forschungsergebnisse zeigen nicht eindeutig, dass eine niedrige Selbstkontrolle einen individuellen Risikofaktor für die Ausübung von Cyberstraftaten dar-stellt, deuten aber auch nicht auf das Gegenteil hin. (Maimon & Louderback, 2019).

Im Fall der Cyberkriminalität sind individuelle Charakteristika möglicherweise nicht so bedeutend, da bei der Cyberkriminalität nur ein minimales Maß an (oder gar keine) Interaktion zwischen Täter und Opfer erforderlich ist. Beim Einsatz von Schadsoftware ist es beispielsweise schwierig zu bestimmen,

wer letztendlich Opfer der Schadsoftware wird, da potenziell jeder Computer unabhängig von den individuellen Charakteristika der Beteiligten infiziert werden kann (Ngo & Paternoster, 2011).

Auf der anderen Seite scheint der Grad der Selbstkontrolle sehr wohl das Risiko zu beeinflussen, Opfer zu werden. Schreck, Stewart und Fisher (2006 *cit in* McNeeley, 2015) stellen eine Verbindung zwischen niedriger Selbstkontrolle und einer geringeren Neigung risikoreiches Verhalten zu vermeiden her (zum Beispiel die Teilnahme an kriminellen Aktivitäten und Kontakt zu gesellschaftlichen Außenseitern), sogar nach persönlichen Viktimisierungserfahrungen. Turanovic and Pratt (2014 *cit in* McNeeley, 2015) bestätigen diese Verbindung zwischen niedriger Selbstkontrolle und wiederholter Viktimisierung: Menschen mit niedriger Selbstkontrolle ändern ihr Leben seltener, selbst nachdem sie Opfer einer Straftat wurden.

HIGHLIGHT | WICHTIGSTE INFORMATION:

Einige Studien über Cyberkriminalität, besonders solche über Straftaten, deren Ausübung direkt von Cybertechnologie abhängt, identifizierten **individuelle Risikofaktoren im Zusammenhang mit Täterschaft**:

- Es gibt Studien, die im Zusammenhang mit Straftaten, deren Ausübung direkt von Cybertechnologie abhängt, festgestellt haben, dass die meisten Täter **relativ geringe technische Kenntnisse** haben (NCA, 2016 *cit in* Maimon & Louderback, 2019).
- Andere wiederum bringen Cyberkriminalität mit **psychologischen und kognitiven Charakteristika** wie Neugierde, kreativem Denken, Problemlösungskapazität und systematischem und technischem Denken in Verbindung (Rogers, 2006, Steinmetz, 2015 *cit in* Maimon & Louderback, 2019).

Andere Verfasser (Morris, 2011 *cit in* Maimon & Louderback, 2019) weisen darauf hin, dass Cyberkriminelle, besonders im Zusammenhang mit Straftaten, deren Ausübung direkt von Cybertechnologie abhängt, **eindeutig externe Kausalzusammenhänge** erfinden, wie Techniken der Neutralisierung oder Rationalisierung, das Leugnen der Existenz des Opfers, des Cyber-Verbrechens und/oder der eigenen Verantwortlichkeit dafür und/oder für die Tatsache verantwortlich zu machen, dass das Cyber-Verbrechen verübt werden konnte.

Bei Hackerangriffen unterscheiden Van der Hulst and Snow (*cit in* Koops, 2010) zwischen 3 verschiedenen Hackertypen, abhängig von deren jeweiliger Motivation:

- junge, männliche Straftäter, die aus Spaß, Neugierde oder weil sie sich den Respekt Gleichaltriger erarbeiten wollen, Cyber-Verbrechen verüben;
- ideologische Hacker, die sehr intelligent und lernbereit sind, von denen einige zu zwanghaftem und antisozialem Verhalten neigen;
- finanziell motivierte Hacker.

3.1.2. Cyberkriminalität als rationale Entscheidung

In der neoklassischen Kriminologie gibt es einen völlig gegensätzlichen Ansatz, der Straftaten als Ergebnis rationaler, kognitiver Prozesse der Reflektion und Entscheidungsfindung durch die jeweiligen

Täter sieht. Das bedeutet, eine Straftat ist eine **rationale Entscheidung des Täters**, der die Kosten und Nutzen der Tat abwägt und dessen Entscheidungen von den gleichen analytischen und reflektierenden Prozessen beeinflusst und getroffen werden (Cornish & Clarke, 1986 *cit in* Yar & Steinmetz, 2019).

Erscheinen dem potenziellen Täter die Kosten einer Straftat, welche die Wahrscheinlichkeit/das Risiko einer Festnahme und der entsprechenden rechtlichen Konsequenzen einschließen im Vergleich zum Gewinn oder den Vorteilen, die er ggf. aus der Verübung der Straftat zieht, als niedrig, steigt gemäß diesem Ansatz die Wahrscheinlichkeit, dass die Straftat verübt wird (Nagin, 1998 *cit in idem*).

Ausgehend von dieser Interpretation könnte die Intensivierung der **erkennbaren Kosten im Zusammenhang mit der Verübung einer Straftat** und/oder die Reduzierung der möglichen **Vorteile, Gewinne oder des Nutzens aus deren Verübung** zur Verhinderung von Straftaten beitragen (Cornish & Clarke, 1986 *cit in idem*).

Studien wie die von Louderback & Antonaccio (2017) weisen darauf hin, dass reflektive kognitive Prozesse das Risiko, in eine Straftat involviert zu sein, reduzieren oder erhöhen können. Diese Annahme basiert auf der Tatsache, dass **Cyberkriminalität als eine Wahl angesehen wird**, bei der vor der Ausübung der Tat eine rationale Beurteilung der Mühen, Kosten und Ergebnisse, die von einem bestimmten Verhalten erwartet werden, durchgeführt wird. (Cornish, 1993 *cit in* Maia et al., 2016).

Einige Studien, die diesem Erklärungsansatz der Cyberkriminalität folgen, (z. B. Bachmann, 2008, Hutchings, 2013 *cit in* Yar & Steinmetz, 2019) weisen darauf hin, dass der Cyberkriminelle bei der Auswahl seiner Ziele und bei der Frage, ob er Risiken eingeht, tatsächlich rationale Entscheidungen trifft.

Dieser rationale Entscheidungsprozess findet selbst dann statt, wenn offensichtlich die Möglichkeit besteht, dass das Opfer Konsequenzen, die mit der Verübung von Cyber-Verbrechen einhergehen und die als Abschreckung dienen sollen, in die Wege leiten kann. Dies führt zu einer Modifizierung der Vorgehensweise, aber nicht unbedingt zur Unterlassung (e.g. Maimon et al., 2013 *cit in idem*).

3.1.3. Die Lifestyle-Theorie

Die **Lifestyle-Exposure-Theorie** von Hindelang, Gottfredson und Garofalo (1978 *cit in* Phillips, 2015) geht davon aus, dass der Alltag einer Person das Ausmaß beeinflusst, in dem sie Orten und Zeiten mit höherem Kriminalitätsrisiko ausgesetzt ist.

In diesem Sinne entstehen Unterschiede bei der Viktimisierungsrate zwischen verschiedenen demografischen Gruppen exakt aufgrund deren verschiedener Alltagsgestaltungen, einschließlich ihrer täglichen Routinen und beruflichen (einschließlich fachlicher und schulischer oder akademischer Beschäftigung) und Freizeitaktivitäten (Hindelang et al., 1978, p. 241 *cit in* McNeeley, 2015), die die Wahrscheinlichkeit, zu riskanten Zeiten hoch risikobehafteten Personen zu begegnen oder sich an hoch risikobehafteten Orten aufzuhalten, entweder erhöhen oder reduzieren.

Die gleiche Theorie geht davon aus, dass demografische Charakteristika, wie Alter, Geschlecht, Familienstand, sozioökonomischer Status, Bildung und Beruf, den Lebensstil beeinflussen, da sie die sozial konstruierten Rollen, Verhaltensweisen, Aktivitäten und Merkmale vorgeben, die eine Gesellschaft für eine Person mit gewissen Charakteristika als angemessen ansieht.

Entsprechend kann der **Online-Lifestyle einer bestimmten Person**, der soziale Aktivitäten wie Chatten oder Veröffentlichen und/oder Teilen von Inhalten in sozialen Netzwerken, berufliche Aktivitäten wie Kommunikation per E-Mail, Audio-/Videoanrufe und/oder Teilen und Speichern von Dateien in dafür vorgesehenen Clouds und Datenbank-Synchronisierungs-Diensten sowie alltägliche Aktivitäten wie Onlineshopping, Recherche auf Webseiten und Nutzung von Anwendungen beinhaltet, als bestimmender Faktor für das Ausmaß der Gefährdung durch Cyberkriminalität gesehen werden (Van Wilsem, 2011).

Des Weiteren beeinflusst der Lebensstil einer Person auch ihr Risiko, sich an illegalen Aktivitäten zu beteiligen, da er ihr gegebenenfalls Gelegenheit zum Verüben von Straftaten bietet (wahrscheinlich mit Gleichaltrigen, die bereits auf Abwege geraten sind) und gleichzeitig den Kontrollmechanismus durch normale Gleichaltrige und andere schützende Beziehungen aushebelt (McNeeley, 2015).

Für eine breiter angelegte Erklärung von Kriminalität/Viktimisierung kombinierte man die Lifestyle-Theorie mit der Routine-Activity-Theorie, die im Folgenden genauer ausgeführt wird (*idem*).

3.1.4. Routine-Activity-Theoriey

Ausgehend von der Lifestyle-Theorie versucht die **Routine-Activity-Theorie** das Vorkommen von Kriminalität durch die Kombination der folgenden Faktoren zu erklären:

- motivierte Täter;
- passende Ziele/Opfer;
- fehlender Schutz (Cohen & Felson, 1979 *cit in* Maimon & Louderback, 2019).

Ist ein (oder mehrere) dieser drei Faktoren nicht erfüllt, sinkt die Wahrscheinlichkeit einer Straftat (Phillips, 2015).

Im Hinblick auf **Cyberkriminelle** erhöht die Nähe des Opfers zu einem motivierten Cyberkriminellen das Risiko der Viktimisierung (Van Wilsen, 2013 *cit in* Maimon & Louderback, 2019).

HIGHLIGHT | WICHTIGSTE INFORMATION:

Die Motivation für die Verübung eines Cyber-Verbrechens kann **situationsabhängig** sein, wenn unabhängig von jeglichen Persönlichkeitsmerkmalen Stimuli gegeben sind, die zur Verübung eines Cyber-Verbrechens führen können (Briar & Piliavin, 1965 *cit in* Maimon & Louderback, 2019). Diese Stimuli hängen häufig mit

dem Auftreten **gelegenheitsmotivierter Kriminalität** zusammen und bestehen bei Straftaten, deren Ausübung direkt von Cybertechnologie abhängt, u. a. aus Anfälligkeiten des Betriebssystems, dem Fehlen von Überwachungssystemen und/oder der Verfügbarkeit unverschlüsselter Daten. Diese Umstände reduzieren das Risiko des Täters, erwischt zu werden, und erhöhen im Gegenzug die Wahrscheinlichkeit von Cyberkriminalität (Willison & Siponen, 2009 *cit in* Maimon & Louderback, 2019).

Der Täter beurteilt die **Eignung** des Opfers/Ziels anhand seines Werts, seiner Attraktivität, Sichtbarkeit, Beweglichkeit und Zugänglichkeit (Felson, 2002 *cit in* Maia et al., 2016).

Hinsichtlich der Eignung des Ziels sind die Gelegenheiten für Cyberkriminelle aufgrund der Zugänglichkeit und Zahl der Internetnutzer vielversprechender als die für Straftaten in der physischen Welt (Saridakis, Benson, Ezingeard & Tennakoon, 2016).

Die Nutzungszeit von IKT und dem Internet scheinen ein wichtiger Indikator der **Eignung des Ziels** zu sein: Personen, die mehr Zeit mit IKT verbringen, haben ein höheres Risiko, einem Cyber-Verbrechen zum Opfer zu fallen. Die Studie von Wang und Kollegen (2015 *cit in* Maimon & Louderback, 2019) zeigt, dass die Zugänglichkeit, Sichtbarkeit und Verfügbarkeit eines Ziels das Risiko von Cyber-Viktimisierung erhöhen. Ebenfalls im Hinblick auf die **Eignung** tritt Cyberkriminalität häufiger in wohlhabenden Ländern auf, da es dort mehr Internetnutzer gibt (Kigerl, 2012 cit in Maimon & Louderback, 2019).

Auch Unternehmen und Organisationen sind gefährdeter, Opfer von Cyberkriminalität zu werden, je geeigneter sie als Ziel sind. Daher passiert Cyberkriminalität häufiger während der Arbeitszeiten des Zielunternehmens oder der Zielorganisation, da zu dieser Zeit mehr potenzielle Opfer verfügbar sind (Kigerl, 2012 *cit in* Maimon & Louderback, 2019).

Im Gegenzug bieten die folgenden Instanzen **Schutz** vor Cyberkriminalität bzw. Straftaten, deren Ausübung direkt von Cybertechnologie abhängt (Grabosky, 2016 *cit in* Maimon & Louderback, 2019):

- Polizeibehörden;
- Regierungsorganisationen, die für die Verwaltung und Überwachung des Cyberspace zuständig sind;
- Internetdienstanbieter, Unternehmen und Branchen, die verschiedene Tools und Verfahren nutzen, um Cyberkriminalität zu verhindern.

In Bezug auf Cyberkriminalität kann dieser Schutz aus verschiedenen Perspektiven analysiert werden (Bossler & Holt, 2009, Holt & Bossler, 2013 *cit in* Maimon & Louderback, 2019). Nämlich:

- Die Abwesenheit eines **sozialen Vormunds** (z. B. elterliche Aufsicht, wenn ein Kind das Internet nutzt) scheint mit einer erhöhten Wahrscheinlichkeit von Cyberkriminalität einherzugehen;

- **Physischer Schutz** (einschließlich der Verwendung von IKT-Sicherheitssystemen oder -software) wird mit der Reduzierung des Risikos der Cyber-Viktimisierung in Verbindung gebracht, auch wenn dieser Ansatz nicht allgemein anerkannt ist;
- **Persönlicher Schutz** (durch Wissen und Fertigkeiten im Bereich ICT und Internetnutzung) reduziert Cyberkriminalität.

Zusammenfassend vertreten die Lifestyle-Theorie und die Routine-Activity-Theorie den Ansatz, dass **die Gewohnheiten und der Alltag einer Person ihre Eignung als (potenzielles) Ziel von Cyberkriminalität beeinflussen und damit ihr Risiko steigern können**, und dass ihre Verfügbarkeit für Täter das Risiko erhöht, Cyberkriminalität zum Opfer zu fallen, besonders in Abwesenheit von Schutzmechanismen. (Cohen, Kluegel & Land, 1981 *cit in* Phillips, 2015).

3.1.5. Weitere relevante Ansätze

Die **Theorie des sozialen Lernens** besagt, dass kriminelle Verhaltensweisen wie alle anderen Verhaltensweisen erlernt werden.

Dieser Lernprozess beinhaltet:

- Interaktionen eines Individuums mit anderen in einer bestimmten Gruppe
- Einstellung eines Individuums zu einer bestimmten Handlung, einschließlich der Techniken, rationalen Gründe und Motivation für die Handlung;
- Nachahmung, einschließlich Beobachtung und Wiederholung einer bestimmten Verhaltensweise, eines anderen Mitglieds der Gruppe;
- Verstärkung, einschließlich positiver Anreize, die die Aufnahme und Erhaltung einer Verhaltensweise fördert.

(Akers, 1998 *cit in* Marcum et al., 2014)

Die Theorie des sozialen Lernens kann auch als Erklärung für Cyberkriminalität herangezogen werden, da sie kriminelles Verhalten als durch die Nachahmung von Gleichaltrigen und die Etablierung positiver Verstärkungsmechanismen als erlernt ansieht, und **Verbindung mit Gleichgesinnten** scheint mit der Ausübung cyberkrimineller Handlungen in Verbindung zu stehen (Hutchings & Clayton, 2016 *cit in* Maimon & Louderback, 2019).

Es lässt sich eine Entwicklung von individuellen Ansätzen oder Perspektiven, die sich auf psychologische und emotionale Charakteristika und kognitive Prozesse eines Individuums konzentrieren, zu deren zwischenmenschlichen Beziehungen. In Bezug auf diese sollte die **Zugehörigkeit zur mehr oder weniger organisierten Netzwerken Gleichgesinnter im Deep Web** mit deren eigener Subkultur und (hierarchischen) Struktur als Risikofaktor für die Verübung von Cyber-Verbrechen hervorgehoben werden

(Macdonald & Frank, 2017 cit *in idem*). Einige Studien deuten darauf hin, dass das Pflegen der **Loyalität in Beziehungen** eine Motivation für die Beteiligung an Cyberkriminalität sein könnte, besonders im Fall von Straftaten, deren Ausübung direkt von Cybertechnologie abhängt (Hutchings & Clayton, 2016 cit *in idem*).

Cyberkriminalität kann auch mithilfe der folgenden drei Dimensionen erklärt werden (Thornberry, Krohn, Lizotte & Chard-Wierschem, 1993 cit *in* Peterson & Densley, 2017):

- **Selektion**: Das Internet an sich ist nicht die Ursache von Cyberkriminalität, viel mehr die individuellen Risikofaktoren und kriminelle Neigung der Personen, die das Internet, IKT und soziale Netzwerke nutzen;
- **Vereinfachung**: Das Internet und IKT vereinfachen aufgrund einiger praktischer Funktionen der Onlinewelt, wie Anonymität, fehlende Schutzmaßnahmen und Gruppenprozesse (wie Konformität gegenüber Gruppennormen) cyberkriminelle Handlungen;
- **Verstärkung**: Die Kombination der zuvor aufgeführten Effekte – Selektion und Vereinfachung – erklärt, dass das Auftreten von Cyberkriminalität mit den **individuellen Risikofaktoren der Personen, die am ehesten zu cyberkriminellen Handlungen neigen**, und den zuvor genannten **Eigenschaften des Internets**, sozialer Netzwerke und IKT zusammenhängt, die die ohnehin vorhandene, kriminelle Neigung verstärken.

3.2. Das Opfer von Cyberkriminalität und die Risikofaktoren für Cyber-Viktimisierung

Wie in Kapitel 1 des Handbuchs bereits ausgeführt, umfassen die Umgebung und verschiedenen Erscheinungsformen der Cyberkriminalität einen häufig als sekundär angesehenen oder außer Acht gelassenen Teil des Verständnisses des kriminellen Phänomens: die **Opfer der Straftaten**.

HIGHLIGHT | WICHTIGSTE INFORMATION:

Entsprechend der Richtlinie 2012/29/EU des Europäischen Parlaments und des Rats vom 25. Oktober 2012 über Mindeststandards für die Rechte, Unterstützung und den Schutz von Opfern von Straftaten[66] ist ein *Opfer* folgendermaßen definiert:

i. *eine natürliche Person, die eine körperliche, geistige oder seelische Schädigung oder einen wirtschaftlichen Verlust, der direkte Folge einer Straftat war, erlitten hat;*
ii. *Familienangehörige einer Person, deren Tod eine direkte Folge einer Straftat ist, und die durch den Tod dieser Person eine Schädigung erlitten haben.*

In anderen Worten handelt es sich beim Opfer einer Straftat um eine Person, die in Folge eines Verstoßes gegen geltende Strafgesetze einen Angriff auf ihr Leben oder physische oder geistige Gesundheit, emotionales Leid oder materiellen Verlust erlitten hat Der Opferbegriff umfasst auch nahe Verwandte oder Abhängige des direkten Opfers sowie Personen, die Schaden erlitten haben, weil sie dem Opfer zu Hilfe zu kommen oder die Tat zu verhindern versuchten.

[66] Das vollständige Dokument ist abrufbar unter: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32012L0029&from=PT

3. KRIMINOLOGISCHE UND VIKTIMOLOGISCHE ANSÄTZE ZUM VERSTÄNDNIS VON CYBERKRIMINALITÄT

Laut dem *IVOR Bericht: Implementing Victim-Oriented Reform of the criminal justice system in the European Union*,[67] einem Bericht, der die Forschung und wissenschaftli-che wie empirische Erkenntnisse über die praktische Umsetzung von Opferrechten in Europa beleuchtet, trägt eine klare, rechtliche Definition des Konzepts Opfer einer Straftat nicht nur zu besserer Unterstützung und Schutz der Opfer bei, sondern fördert auch **das Bewusstsein und die Anerkennung des Opferstatus'** bei der Betrachtung des kriminellen Phänomens und im Justizsystem.

An dieser Stelle wollen wir Opfer sichtbar machen, die als Folge einer (oder mehrerer) Straftaten, deren Ausübung direkt von Cybertechnologie abhängt, und/oder jeglicher Straftat, die durch das Internet oder IKT vereinfacht wurde, einen physischen, moralischen, geistigen, emotionalen oder materiellen Schaden erlitten haben. Zuerst widmen wir uns den Risikofaktoren, die im Hinblick auf Cyberkriminalität existieren.

Risikofaktoren[68] sind Charakteristika, Umstände oder Variablen einer Person, die die Wahrscheinlichkeit einer negativen oder unerwünschten Entwicklung erhöhen (Reppold et al., 2002 *cit in* Maia et al., 2016).

Sie können sowohl statisch als auch dynamisch sein. Statische Charakteristika oder Umstände einer Person und/oder ihrer Vergangenheit können nicht geändert werden, wie zum Beispiel Geschlecht, persönliche Erfahrungen mit Gewalt in der Kindheit oder der Verlust eines Verwandten. Dynamische Risikofaktoren hingegen umfassen Charakteristika, Umstände oder Variablen, die verändert werden können und die Wahrscheinlichkeit des Auftretens eines bestimmten Problems erhöhen.

Die Konzeptualisierung von Cyberkriminalität als ein Problem oder negatives Ergebnis macht Charakteristika oder Umstände einer Person, die ihre Anfälligkeit für Cyber-Viktimisierung steigern, zu **Risikofaktoren**.

Die Forschung in diesem Bereich steckt, wie viele weitere, die das Verständnis von Cyberkriminalität untersuchen, noch in den Kinderschuhen. Die folgenden Studien sollten berücksichtigt werden.

3.2.1. Risikofaktoren in Zusammenhang mit sozio-demografischen Charakteristiken

Es gibt keine eindeutige Verbindung zwischen dem **Geschlecht** und dem Risiko für Cyber-Viktimisierung. An dieser Stelle können, ohne die verschiedenen Formen der Cyberkriminalität in Betracht zu ziehen, keine Erkenntnisse gewonnen werden. Es folgt eine Analyse der verfügbaren Informationen.

Einige Studien deuten darauf hin, dass Frauen wahrscheinlicher Opfer von Cyber-Verbrechen werden, obwohl es hierzu keinen allgemeinen Konsens gibt (Bossler & Holt, 2009, 2010, Ngo & Paternoster, 2011 cit in *Maimon* & Louderback, 2019). Das gleiche scheint für Cyberstalking und Cybermobbing (Holt & Bossler, 2008) zu gelten, bei denen der Frauenanteil unter den Opfern größer ist.

Im Hinblick auf den sexuellen Missbrauch und die sexuelle Ausbeutung von Kindern im Internet

[67] Zusätzliche Informationen über die Reflektion des Konzepts des Opfers einer Straftat und anderer Themen, die in Verbindung mit deren Rechte und ihrer effektiven Umsetzung stehen, können im Gesamtbericht nachgelesen werden, unter https://apav.pt/publiproj/images/yootheme/PDF/IVOR-Repot-WebVersion.pdf .

[68] An dieser Stelle muss darauf hingewiesen werden, dass das Konzept der Risikofaktoren nicht losgelöst vom Konzept der **Schutzfaktoren** betrachtet werden kann, welches die Charakteristika oder Umstände beschreibt, die die Wahrscheinlichkeit des Auftauchens oder Eintretens eines bestimmten Problems reduzieren.

ist der Anteil weiblicher Opfer zwar ebenfalls größer als der der männlichen, jedoch sind letztere zumindest in den bekannten Fällen für gewöhnlich das Ziel schwerwiegenderer, übergriffigerer und stärkerer Formen sexueller Aggression[69].

In Bezug auf den Kontakt mit Hassrede im Internet sind die Unterschiede zwischen Kindern und Jugendlichen beider Geschlechter in Europa im Durchschnitt minimal. Auch was den Erhalt selbst produzierter sexueller/Sexting-Inhalte betrifft, wurden für beide Geschlechter sehr ähnliche Durchschnittswerte ermittelt[70].

In den bisher durchgeführten Studien konnte keine eindeutige Verbindung zwischen dem **Alter** und dem Risiko für Cyber-Viktimisierung festgestellt werden (Bossler & Holt, 2009, Ngo & Paternoster, 2011 cit *in Maimon* & Louderback, 2019). Allerdings deuten einige Studien darauf hin, dass ältere Menschen öfter Opfer von Straftaten, deren Ausübung direkt von Cybertechnologie abhängt, werden, wie zum Beispiel Hackerangriffe, als andere Erwachsene (Leukfeldt & Yar, 2016 cit *in Maimon* & Louderback, 2019).

Wie im Folgenden weiter ausgeführt, nutzen jüngere Menschen IKT und das Internet viel intensiver, besonders die sozialen Netzwerke, was verglichen mit älteren und weniger engagierten Nutzern zu einem höheren Risiko für Cyber-Viktimisierung führt (Staksrud, ÓLafsson & Livingstone, 2013 cit *in Näsi*, Oksanen, Keipi & Räsänen, 2015; Näsi et al., 2015).

Es gibt Studien, die darauf hindeuten, dass es eine negative Verbindung zwischen dem **Bildungsniveau** und dem Risiko für Cyber-Viktimisierung, zum Beispiel durch Hackerangriffe, gibt, d. h. ein höheres Bildungsniveau wird mit einem niedrigeren Risiko für Cyber-Viktimisierung in Verbindung gebracht (van Wilsem, 2013 *cit in* Maimon & Louderback, 2019). Ähnlich wie bei den soziodemografischen Charakteristika und in Anbetracht der Erkenntnisse über den Einfluss individueller Charakteristika auf das Risiko für Cyber-Viktimisierung ist der Effekt dieses Risikofaktors weiter zu untersuchen.

3.2.2. Risikofaktoren in Zusammenhang mit der Nutzung des Internets und IKT

Das Konzept der **Technikkompetenz** umfasst das Bewusstsein, Wissen und die Fähigkeiten, die es einer Person ermöglichen, das Internet und IKT sowie die damit in Verbindung stehende Ausrüstung und Werkzeuge effektiv zu nutzen und sich in digitaler Umgebung zurechtzufinden (Holt & Bossler, 2013 cit *in Maimon* & Louderback, 2019).

Entsprechend ist sie ein wichtiger Faktor bei der Feststellung der Gefährdungs- und Schutzlevel in Zusammenhang mit Cyber-Viktimisierung. Kompetenz im Umgang mit dem Internet und IKT scheint das Risiko für Cyber-Viktimisierung zu reduzieren, da der Nutzer durch sie über die Fähigkeit verfügt, Situationen, in den seine Sicherheit gefährdet sein könnte, zu identifizieren und entsprechend zu handeln (Holt & Bossler, 2008).

Verschiedene Studien deuten darauf hin, dass die **Nutzungshäufigkeit von Internet und IKT**

[69] Ausführliche Informationen sind abrufbar unter https://www.interpol.int/Crimes/Crimes-against-children/International-Child-Sexual-Exploitation-database .

[70] Die Ergebnisse der EU Kids Online 2020: *Survey results from 19 countries* sind abrufbar unter https://www.eukidsonline.ch/files/Eu-kids-online-2020-international-report.pdf .

die Anfälligkeit für Cyber-Viktimisierung durch verschiedene Formen der Cyberkriminalität, wie Hackerangriffe, Einsatz von Schadsoftware oder Phishing, erhöht (Yucedal, 2010; Leukfeldt & Yar, 2016; Reyens, 2015 *cit in* Maimon & Louderback, 2019). Es scheint einen Zusammenhang zwischen der Nutzungshäufigkeit von IKT und Viktimisierung durch Cyber-kriminalität zu geben: Personen, die in ihrem Alltag häufiger soziale Netzwerke und IKT nutzen, setzen sich einem erhöhten Risiko aus, Opfer von Cyberkriminalität zu werden (Butler, 2013). Diese Ergebnisse entsprechen den Annahmen der kriminologischen Theorien, die in diesem Handbuch bereits erörtert wurden.

HIGHLIGHT | WICHTIGSTE INFORMATION:

Das erhöhte Risiko der Cyber-Viktimisierung als Folge der Nutzung von IKT darf nicht linear interpretiert werden, da die Nutzung des Internet und IKT an sich nicht das Risiko für Cyber-Viktimisierung erhöht.

Dies geschieht vielmehr durch die **Verhaltensweisen und Art der Aktivitäten während der Nutzung von IKT und dem Internet**, die die ausschlaggebenden Faktoren für das gesteigerte Risiko sind (Butler, 2013; Holt & Bossler, 2008).

Dieses Risiko wird im nächsten Kapitel dieses Handbuchs genauer ausgeführt.

3.2.3. Riskante Verhaltensweisen und ihre Verbindung zu Cyber-Viktimisierung

HIGHLIGHT | DATEN IM FOKUS:

Laut den Ergebnissen der o. g. transnationalen Studie *Health Behaviour in Schoolaged Children* bezeichneten sich 35 % befragten Schüler als **intensive Internet- und IKT-Nutzer**, d. h. sie nutzen diese Anwendungen täglich und für einen signifikanten Zeitraum.

Außerdem nutzt 1 von 10 Schülern das Internet intensiv für Kommunikation mit Personen, die er oder sie ausschließlich online kennen.

Im Durchschnitt zeigten 7% Schüler **Anzeichen von Suchtverhalten** in Verbindung mit der Nutzung des Internets und IKT, besonders die weiblichen Befragten.

Wie bereits in Zusammenhang mit der Lifestyle-Theorie und der Routine-Activity-Theorie (s. Kapitel 3.1 dieses Handbuchs) festgestellt, beeinflusst das Onlineverhalten einer Person ihr Risiko, Opfer eines Cyber-Verbrechens zu werden (Yucedal, 2010).

Wie bereits in den kriminologischen Theorien dargelegt, beinhaltet das Online-Verhalten alle **Arten**

von Aktivitäten, die im Internet oder über das Internet und IKT stattfinden, entweder in Form von sozialer Interaktion und Freizeitaktivitäten, Handlungen und Aufgaben im beruflichen, erzieherischen oder anderen Kontext und sogar Routineaufgaben wie Onlineshopping, Onlinebanking, die Buchung von Terminen und/oder die Erfüllung behördlicher Anforderungen. Die Häufigkeit und Intensität der Internet- und IKT-Nutzung spielt ebenfalls eine Rolle.

Unter Anwendung des umfassenden Konzepts des Onlineverhaltens wird klar, dass das Risiko für Cyber-Viktimisierung von den Handlungen abhängt, die im oder über das Internet und IKT erfolgen, und von der täglichen Routine.

Einige Handlungen, wie das Herunterladen von Gratis-Software[71] oder die Nutzung von File-Sharing-Webseiten, bergen ein höheres Risiko für Cyber-Viktimisierung als andere, wie E-Mails oder Nachrichten lesen. Analog dazu werden Personen, die unsicheren Online-Aktivitäten nachgehen, wie zum Beispiel unbekannte Webseiten besuchen und/oder Musik, Videos, Filme und/oder Spiele von illegalen Webseiten herunterladen, werden leichter das Ziel einer Form der Cyber-Viktimisierung (Choi, 2008, Moitra, 2005, Yar, 2005, 2006 *cit in* Yucedal, 2010). Die Verwendung einer Webcam, häufiges Onlineshopping und das Annehmen von Freundschaftsanfragen Unbekannter in den sozialen Netzwerken erhöhen das Risiko für Cyber-Viktimisierung im Vergleich zu Personen ohne solche Online-Angewohnheiten (Clarke, 2004 Van Wilsem, 2011; Butler, 2013).

HIGHLIGHT | WICHTIGSTE INFORMATION:

In Hinblick auf das Online- und Internetnutzungsverhalten sollte ebenfalls darauf hinge-wiesen werden, dass **Personen mit persönlicher Erfahrung im Bereich Täterschaft oder Beteiligung an Cyberkriminalität ebenfalls einem erhöhten Risiko der Cyber-Viktimisierung ausgesetzt sind** (Choi, 2008, Wolfe et al., 2008, Bossler & Holt, 2009, Van Wilsen, 2013 cit *in Maimon* & Louderback, 2019).

Das erhöhte Viktimisierungsrisiko von Personen, die in illegale Aktivitäten verwickelt sind, tritt auch bei *herkömmlicher* Kriminalität auf und wird dem Lebensstil, Verhalten und Kontakt zu gefährdenden Umständen, Kontexten und Personen/Gruppen zuge-schrieben (s. Zusammenfassung kriminologischer Theorien in Kapitel 3.1 dieses Handbuchs).

Sowohl bei herkömmlicher als auch Cyberkriminalität wird die Beteiligung und Zugehörigkeit zu spezifischen, kriminellen Subkulturen sowohl mit dem Risiko der Täterschaft (Macdonald & Frank, 2017 cit *in Maimon* & Louderback, 2019) als auch mit dem der Viktimisierung, in erster Linie durch den Kontakt zu Gleichgesinnten, in Verbindung gebracht.

Um die Relevanz des Verhaltens bei der Internet- und IKT-Nutzung und seine Verbindung mit der Anfälligkeit für Cyber-Viktimisierung besser zu verstehen, muss der **Enthemmungseffekt** einbezogen werden, der ein wichtiges Merkmal der Internet- und IKT-Nutzung ist. Der Enthemmungsprozess oder -effekt entsteht aus den Auswirkungen, die physische Distanz auf Interaktion oder Kommunikation hat. Die Abwesenheit direkten Kontakts im Kommunikationsprozess, die größere Anonymität und der Eindruck größerer Kontrolle über den Interaktionsprozess scheinen dazu beizutragen,

[71] Gratis-Software bezeichnet Software oder Computerprogramme für deren Verwendung keine Lizenz oder Bezahlung erforderlich ist.

dass Informationen leichter geteilt und Emotionen und Gedanken freier ausgedrückt werden und Verhaltensweisen auftreten, die bei Interaktion im konventionellen Kontext nicht geteilt, ausgedrückt oder umgesetzt würden (Suler, 2004; Martellozzo & Jane, 2017). Dieser scheinbar vorteilhafte Enthemmungseffekt kann dazu beitragen, dass eine Person leichter in Situationen gerät und/oder Online-Verhaltensweisen adaptiert, die ihr Risiko für Cyber-Viktimisierung erhöhen (Agustina, 2015).

HIGHLIGHT | ANGEBOTE IM FOKUS:

Eine Arbeitsgruppe eines US-amerikanischen Unternehmens entwickelte 1995 eine als *Netiquette Guidelines* bezeichnete Erklärung, in der zum ersten Mal das Konzept einer ***Netiquette*** beschrieben wurde. Sie bestand aus einer Reihe von Verhaltensregeln, einschließlich Kommunikationsregeln und Sicherheitsstandards, für Personen und Zusammenschlüsse und sollte eine sichere und angemessene Nutzung des Internets und seiner verschiedenen Kommunikationswerkzeuge ermöglichen.

Das Originaldokument ist abrufbar unter https://www.ietf.org/rfc/rfc1855.txt .

In dieser Hinsicht ist die Wichtigkeit des **Bewusstseins, Wissens** und der **Kontrolle** über die **Art und Weise, wie persönliche Informationen** im Internet und besonders in den sozialen Netzwerken geteilt werden. Es konnte ein Zusammenhang zwischen der persönlichen Risikowahrnehmung, der Kontrollwahrnehmung hinsichtlich geteilter Informationen und dem Verhalten beim Teilen von Informationen in den sozialen Netzwerken festgestellt werden: Je mehr Kontrolle Personen über geteilte oder teilbare Informationen zu haben glauben, desto vorsichtiger gehen sie mit diesen Informationen um, desto sicherer fühlen sie sich und desto niedriger ist ihr Risiko, Opfer von Cyberkriminalität zu werden (Hajli & Lin, 2014 cit *in* Saridakis et al., 2016).

3.3. Kollektive Entitäten als Ziele von Cyberkriminalität

Cyberkriminalität kann ebenso kollektive Entitäten betreffen und überschreitet damit die Grenzen der individuellen Viktimisierung, wie sie in diesem Handbuch erörtert wird.

Damit beziehen wir uns auf Situationen, in denen **Unternehmen, Großkonzerne, Institutionen und sogar Regierungsinfrastrukturen** Ziele von Cyberkriminalität werden (Yucedal, 2010; Näsi et al., 2015).

Cyberkriminalität kann solchen Entitäten enormen Schaden zufügen, sei es durch den Verlust von Kunden und/oder Kompromittierung oder Diebstahl vertraulicher Informationen, durch unmittelbare finanzielle Verluste, die sogar einzelne Kunden betreffen können oder langfristige Verluste durch einen Vertrauensverlust der Kunden in das Produkt/die Dienstleistungen des Unternehmens (Nykodym, Taylor & Vilela, 2005, 2005; Kratchman et al., 2008).

3. KRIMINOLOGISCHE UND VIKTIMOLOGISCHE ANSÄTZE ZUM VERSTÄNDNIS VON CYBERKRIMINALITÄT

HIGHLIGHT | WICHTIGSTE INFORMATION:

Nehmen Cyberkriminelle kollektive Entitäten ins Visier, spielt die menschliche Komponente eine wichtige Rolle. Genauer gesagt, die **Aufgaben der Fachkräfte und Mitarbeiter** solcher Organisationen und deren **jeweiliger Anteil an Organisations- und Schutzmaßnahmen** gegen Cyberkriminalität, ebenso wie ihre persönlichen Schutzmaßnahmen gegen Cyberkriminalität.

Es ist nachgewiesen, dass sich Fachkräfte und Mitarbeiter eher an die Schutzmaßnahmen und -Richtlinien des Unternehmens oder der Organisation halten, wenn sie sich der Anfälligkeiten der Organisationsstruktur bewusst sind (Johnston & Warkentin, 2010 cit *in Maimon* & Louderback, 2019; Siponen et al., 2010 cit in *Maimon* & Louderback, 2019).

Der in Kapitel 1 dieses Handbuchs näher betrachtete Cyberterrorismus ist ein Beispiel für Cyberkriminalität gegen kollektive Entitäten, da er wie oben beschrieben auf die Zerstörung und/oder Lahmlegung für das Funktionieren einer Gesellschaft oder eines Staates notwendiger Infrastrukturen abzielt und nicht unbedingt auf den Schaden eines einzelnen Bürgers (was im Zuge des Angriffs trotzdem passieren kann).

In dieser Hinsicht soll auf das Konzept des Hacktivism hingewiesen werden, welches eine Verbindung aus politischem Aktivismus und IKT ist, bei der Hackerangriffe politischen Zwecken oder Kampagnen dienen (Yar & Steinmetz, 2019).

HIGHLIGHT | WICHTIGSTE INFORMATION:

Die international agierende, dezentralisierte Hacktivism-Bewegung Anonymous, die in den 2000er Jahren entstand und für ihre *Hackerangriffe* und DDoS (siehe Kapitel 1.3 dieses Handbuchs für weitere Informationen über diese Formen der Cyberkriminalität) bekannt ist, wurde mit verschiedenen Angriffen auf Regierungsinfrastrukturen, Großkonzerne, Fi-nanzinstitutionen und religiösen Organisationen in Verbindung gebracht.

Die Ziele dieser Bewegung sind nicht eindeutig, aber sie behaupten, gegen Zensur und Unterdrückung und für das Recht auf freie Meinungsäußerung zu kämpfen.

4. KOSTEN UND AUSWIRKUNGEN DER CYBERKRIMINALITÄT

Die in diesem Abschnitt vorgenommene Erörterung der Symptome und Indikatoren der Auswirkungen von Cyberkriminalität kann aufgrund der verschiedenen Ausprägungen und des breiten Umfangs nur unter Vorbehalt erfolgen. Die u. g. Folgen sind stets reduktiv und generisch zu betrachten und berücksichtigen nicht die Individualität der einzelnen und persönlichen Cyber-Viktimisierungserfahrung.

Auch die finanziellen und ökonomischen Auswirkungen der Cyberkriminalität werden erläutert. Obwohl Cyber-Verbrechen häufig direkt und/oder indirekt einzelne Opfer betreffen, spiegeln sich die daraus entstehenden Kosten auch in den Kosten kollektiver Entitäten wider, welche attraktive Ziele für Cyberkriminalität sind.

4.1. Die Opfer von Cyberkriminalität und die Folgen einer Cyber-Viktimisierungserfahrung

Die Auswirkungen von Cyberkriminalität auf das Opfer fallen sehr unterschiedlich aus, da sie von einer Reihe von Faktoren verstärkt oder abgeschwächt werden:

- **Individuelle Faktoren** wie sozio-demografische Merkmale und Internetkompetenz (beschrieben in Kapitel 3 dieses Handbuchs über die Risikofaktoren für Cyber-Viktimisierung);
- **Faktoren im Hinblick auf das Cyber-Verbrechen** selbst, einschließlich der Art des Verbrechens, dem Aggressionsniveau, der Dauer der Viktimisierung, dem Verbreitungsniveau oder dem Grad der Öffentlichkeit der Viktimisierung und gegebenenfalls die Beziehung zum Täter (z. B. Cyber-Viktimisierung in zwischenmenschlichen Beziehungen);
- **Faktoren im Hinblick auf das Unterstützungsnetzwerk**, einschließlich des formalen Unterstützungsnetzwerks (d. h. die Ressourcen des Justiz-, Gesundheits- und Sicherheitssystems, des Systems der sozialen Absicherung und ziviler Organisationen) sowie des informalen Unterstützungsnetzwerks wie Familie und Freunde.

4.1.1. Physische, psychologische und emotionale Folgen

Es gibt nur wenige Studien über die Auswirkungen von Cyber-Viktimisierung und diese konzentrieren sich, mit wenigen Ausnahmen (z. B. Jansen & Leukfeldt, 2018), hauptsächlich auf die Auswirkungen einzelner Formen der Cyberkriminalität, wie zum Beispiel Ver-brechen, die durch das Internet und IKT ermöglicht werden, wahrscheinlich durch ihre zwischenmenschliche oder Beziehungskomponente.

Man geht allgemein davon aus, dass die Folgen, unter denen die Opfer von Cyberkriminalität leiden, sich nicht nennenswert von denen der Opfer sog. *herkömmlicher* Straftaten unterscheiden. Die Folgen und Reaktionen, die häufig genannt werden, sind: Verlust des Selbstvertrauens; Schuld; Scham; Wut und Frustration; Beklemmung; Angst und Traurig-keit; Gefühle der Unsicherheit,

Machtlosigkeit und Enttäuschung (Leukfeldt et al., 2019; Cross et al., 2016; De Kimpe et al., 2020). Die emotionalen Auswirkungen einiger Arten von Cyberkriminalität können ebenso schwerwiegend sein wie die finanziellen Konsequenzen (Modic & Anderson, 2015). Viktimisierung kann die Art und Weise verändern, wie sich die Opfer selbst sehen und welche Bedeutung sie der Welt um sie herum beimessen, einschließlich einer Reduzierung ihres Selbstvertrauens und des Vertrauens in andere (Jansen & Leukfeldt, 2018). Dies kann sogar zu körperlichen Folgen wie Schlaflosigkeit, Übelkeit und/oder Gewichtsverlust führen (Cross et al., 2016).

Häufige emotionale, psychische und verhaltensändernde Folgen von Cyberstalking sind Gefühle der Angst, Verzweiflung und Besorgnis beim Opfer (Holt & Bossler, 2008). Die Angst kann aus der Angst vor den Handlungen des Cyberstalking-Täters entstehen, aber auch die Angst davor sein, den Ruf zu verlieren, weil persönliche oder private Informationen online veröffentlicht werden und als solche ein breites Publikum erreichen könnten. Symptome wie Beklemmung, einschließlich des erneuten Durchlebens des Vorfalls, und Suchtmittelmissbrauch werden ebenfalls mit der Viktimisierung durch Cyberstalking in Verbindung gebracht. Neben den emotionalen und psychischen Folgen können Anzeichen körperlichen Unwohlseins auftreten, einschließlich Somatisierung[72], Schlafstörungen, Müdigkeit oder extreme Schwäche, Appetitlosigkeit, Kopfschmerzen und Übelkeit (Davies, Clark, & Roden, 2016).

Häufige negative Effekte auf das psychische und emotionale Wohlbefinden der Opfer von Cybermobbing sind ein niedriges Selbstbewusstsein, Traurigkeit, Wut, Einsamkeit und Frustration, ebenso wie somatische Störungen, Depressionen und Suizidgedanken. Cybermobbing beeinträchtigt die soziale und schulische Leistungsfähigkeit der Opfer im Kindes- oder Heranwachsendenalter und führt häufig zu einem Gefühl verminderter Leistungsfähigkeit, Isolation, Fehlzeiten und einer Verschlechterung der Noten (Beran & Li, 2007, Kowalski & Limber, 2013 cit in *Arafa*, Mahmoud & Senosy, 2015; Wang et al., 2011 cit in Arafa *et al.*, 2015).

Retrospektive Studien haben ein breites Spektrum negativer Auswirkungen von sexuellem Missbrauch in der Kindheit auf das emotionale und psychische Wohlbefinden festgestellt, einschließlich: Probleme in Schule und Beruf, Aggressivität und Verwicklung in Kriminalität. Ähnlich wie Cybermobbing führen der sexuelle Missbrauch oder die sexuelle Ausbeutung von Kindern zu Symptomen wie Angst, Unwohlsein, Aggressivität, Gereiztheit, Schlafstörungen und rückschrittlichen[73] Verhaltens. Verschlechterte Noten, Fehlzeiten und die Aneignung unangemessenen sexuellen Verhaltens können ebenfalls Folgen sein (Roopesh, 2016 *cit in* APAV, 2019).

Den Fokus auf den sexuellen Missbrauch und die sexuelle Ausbeutung von Kindern sowie deren Folgen[74] zu setzen, sprengt aufgrund der häufig außergewöhnlichen Umstände den Rahmen dieses Handbuchs. Entsprechend finden Sie im Folgenden lediglich eine kurze Zusammenfassung der unangemessenen sexuellen Verhaltensweisen, die aus der Erfahrung sexueller Gewalt entstehen können.

[72] Somatisierung bezeichnet das Auftreten körperliche Symptome als Ausdruck emotionaler und psychischer Probleme ohne offensichtlichen medizinischen/körperlichen Grund.

[73] Rückschrittliches Verhalten bezeichnet Rückschritte in der Entwicklung, die das Kind bereits erreicht hat. Diese können u. a. sein: Bettnässen (unkontrolliertes Urinieren), Enkopresis (unkontrolliertes Einkoten) und Rückschritte in der Sprache/Kommunikation.

[74] Ausführliche weiterführende Informationen über sexuelle Gewalt an Kindern finden Sie hier: APAV (2019). *CARE Handbook - support for children and young people victims of sexual violence (2nd edition revised and expanded)*. Lissabon: APAV.

Tabelle 2: Sexuelle Verhaltensweisen, die eine Folge der Erfahrung sexueller Gewalt sein können

Sexualisierter Ausdruck von Zuneigung

- Unangemessenes Berühren der Sexualorgane anderer Kinder und Heranwachsender (besonders Kinder und Heranwachsende anderer Altersgruppen als der eigenen und/oder zu denen das Kind oder der o-der die Heranwachsende keine bestehende Vertrauensbeziehung hat)
- Exzessives oder unangemessenes Berühren Erwachsener
- Versuche, Erwachsene zu verführen

Früh sexualisierte Sprache

- Verwendung sexueller Ausdrücke, die auf ein für die Altersgruppe ungewöhnlich detailliertes Wissen über Sexualität hindeuten

Zwanghafte Masturbation und/oder extremes autoerotisches Verhalten

- Ständiges Masturbieren, auch wenn dieses ausdrücklich untersagt oder von Erwachsenen verboten wurde (z. B. durch entsprechende Bestrafung)
- Masturbation an öffentlichen Orten und/oder in der Nähe anderer Personen

Inszenierung oder Simulation expliziter sexueller Handlungen und/oder Interaktionen

Sexuelle Verhaltensweisen, die Unwohlsein bei einem selbst oder anderen (besonders Gleichaltrigen) hervorrufen

- Die sexuelle Handlung bereitet dem Täter und der oder dem Gleichaltrigen, mit dem oder der der Täter die sexuelle Handlung ausführt, körperliche Schmerzen.
- Die sexuelle Handlung verletzt die Privatsphäre der oder des Gleichaltrigen, erfolgt gegen seinen oder ihren Willen und führt zu entsprechenden Beschwerden unter Gleichaltrigen

Sexuelle Handlungen als eine Form der Erwiderung oder Anerkennung von Zuneigung und/oder materieller Güter

Ständige Besorgnis über Sexualität

Es steht außer Frage, dass sexueller Missbrauch und sexuelle Ausbeutung von Kindern über das Internet deren Gesundheitsentwicklung, einschließlich der Entwicklung ihrer Sexualität, und Identität beeinträchtigen. Aufgrund des andauernd hohen Viktimisierungsrisikos in Fällen sexuellen Missbrauchs oder sexueller Ausbeutung von Kindern ist es wahrscheinlich, dass die Schwere der Auswirkungen der Erfahrung zunimmt und die Folgen auch im Erwachsenenalter andauern (Frothingham et al., 2000 *cit in* Sigurjonsdottir, 2013).

Hassrede im Internet hat einen Doppeleffekt: Zum einen die Botschaft an das Opfer, zum anderen die zugrundeliegende Botschaft, die die Inhalte transportieren sollen (dass das Opfer und die Gruppe, zu der er oder sie gehört, nicht von der Gesellschaft akzeptiert werden). Die Anonymität des Internets und IKT ermöglicht den Tätern, Online-Aggressionen über einen langen Zeitraum hinweg aufrechtzuerhalten und so das emotionale und psychische Leiden des Opfers zu verlängern. Außerdem trägt Anonymität zur Verstärkung und sozialen „Validierung" bei, besonders wenn die Inhalte in sozialen Netzwerken verbreitet werden, und intensiviert die negativen Auswirkungen auf das emotionale und psychische Wohlbefinden des Opfers und sogar sein Verhalten im sozialen Kontext (McGonagle, 2013).

Bei Straftaten, deren Ausübung direkt von Cybertechnologie abhängt, wie Hackerangriffe, Spamming

oder Internetbetrug, werden die Auswirkungen auf das emotionale und psychische Wohlbefinden stark unterschätzt und daher häufig als Straftaten mit geringen Folgen eingestuft (Button, Lewis, & Tapley (2014a cit *in Jansen* & Leukfeldt, 2018). Einige Studien weisen jedoch darauf hin, dass diese Formen der Cyberkriminalität neben finanziellen Folgen auch emotionale und psychische Symptome wie Angst oder Unwohlsein sowie körperliche Symptome wie Schlafstörungen und Herzrasen verursachen können (Jansen & Leukfeldt, 2018).

4.1.2. Finanzielle Folgen

Der finanzielle Schaden, den Opfer von Cyberkriminalität erleiden, hängt hauptsächlich von der Form der Cyberkriminalität ab, der sie zum Opfer gefallen sind (Butler, 2013).

Cyberkriminalität führt zu einer Reihe von direkten und indirekten Kosten. Bei Letzteren handelt es sich um die Kosten, die dem Opfer als eine Folge des Verbrechens entstehen, wie allgemeiner Zeitverlust, Verlust von Arbeitszeit, erhöhte Ausgaben für die Gesundheit, Kosten für Reisen und Telekommunikation, der Bedarf an neuem IT-Equipment und/oder die Nichterfüllung vertraglicher Vereinbarungen (Leukfeldt et al., 2019). Einige Formen der Cyberkriminalität erfordern, dass das Opfer seinen Alltag verändert. Dies kann zum Beispiel die Einrichtung von Schutzmaßnahmen und die Umsetzung effektiverer Cybersicherheitsmechanismen bedeuten, aber auch fundamentalere Veränderungen im Lebensstil und Alltag, einschließlich eines Umzugs, Job- oder Universitätswechsels oder anderer, die Kosten verursachen.

Die Kosten, die einer Entität entweder für die Prävention oder als Folge von Cyberkriminalität entstehen, erläutert in Abschnitt 4.3 dieses Handbuchs, wirken sich letztendlich wieder auf das Individuum aus: nämlich die Online-Kunden und Nutzer eines Produkts, eines Guts oder einer Dienstleistung (Das & Nayak, 2013).

4.1.3. Die Angst vor Cyberkriminalität und das wahrgenommene Risiko für Cyber-Viktimisierung

Angst vor Kriminalität ist eine emotionale Reaktion auf Kriminalität und/oder Symbole, die damit in Verbindung stehen, während das **wahrgenommene Risiko** eine kognitive Beurteilung ist, mithilfe derer Personen ihr eigenes Viktimisierungsrisiko auf Grundlage ihrer persönlichen Erfahrungen, ihres sozialen Kontexts und Umstände einschätzen, die sich wiederum auf die Angst vor Kriminalität auswirkt (Ferraro, 1995, Rontree, 1998 cit in Yucedal, 2010).

Daraus folgt, dass persönliche Viktimisierungserfahrungen das wahrgenommene Risiko einer (Re-) Viktimisierung und entsprechen die Angst vor Kriminalität verstärken können. Diese kognitiven Prozesse sind nicht zwangsläufig negativ, da sie zu der Umsetzung von Sicherheits- und Schutzmaßnahmen führen können (Rountree & Land, 1996, cit in idem).

Nämlich:

- Eine Person, die bereits Opfer einer Straftat wurde oder sich selbst einem erhöhten Viktimisierungsrisiko ausgesetzt sieht, **setzt mehr sichere und schützende Verhaltensweisen**, einschließlich Einschränkungen sozialer Aktivitäten/Interaktionen oder Veränderungen im Alltag, und setzt eher Schutzmaßnahmen und -mechanismen ein;
- Eine Person, die bereits Opfer einer Straftat wurde, schätzt ihr **Reviktimisierungsrisiko tendenziell höher ein** und hat daher mehr **Angst vor Kriminalität** als Menschen ohne Viktimisierungserfahrung (Hindelang et al., 1978, Cohen & Felson, 1979, Ferraro, 1995, Goodrum, 2007 cit *in idem*).

Diese **kognitiven Prozesse für die Einschätzung des wahrgenommenen Reviktimisierungsrisiko treffen auch auf Cyber-Viktimisierung zu**. Das wahrgenommene Cyber-Viktimisierungsrisiko als Ergebnis einer Analyse der persönlichen Cyber-Viktimisierungserfahrung (sofern vorhanden) und der Hinweise auf Viktimisierung/Kriminalität aus dem Online-Kontext kann zu Verhaltensänderungen führen, die einen besseren Schutz bieten sollen. Dies kann die Umsetzung von Cybersicherheitsmaßnahmen/-mechanismen (wie Antivirensoftware und Firewalls[75]) sowie die Änderung des Internet- und IKT-Nutzungsverhaltens zur Folge haben (Yucedal, 2010).

Letztendlich beeinflusst das wahrgenommene Cyber-Viktimisierungsrisiko auch den Grad der **Anfälligkeit für Cyber-Viktimisierung**, da eine Person, die sich selbst einem Cyber-Viktimisierungsrisiko ausgesetzt sieht, wahrscheinlicher Verhaltensweisen und Maßnahmen umsetzt, die der Sicherstellung der Cybersicherheit dienen, was zu einer Reduzierung des Cyber-Viktimisierungsrisikos beiträgt.

HIGHLIGHT | DATEN IM FOKUS:

Laut dem o. g. Eurobarometer 423 zeigten die Befragten ein **hohes Maß an Besorgnis wegen Cyberkriminalität und ihrer Risikofaktoren**.

Die wichtigsten Ergebnisse waren:

- Die Mehrheit (85% der Befragten) stimmte der Aussage zu, das **Risiko der Cyber-Viktimisierung nehme zu**.
- 73% der Befragten machten sich Sorgen, **dass ihre persönlichen Daten online nicht sicher gespeichert sind**.
- Die Formen der Cyberkriminalität, vor denen sich die Befragten am meisten fürchten, in absteigender Reihenfolge: **Identitätsdiebstahl im Internet** (68%), **Schadsoftware** (66%), **Internetbetrug** (zwischen 56% und 63%), **Hackerangriffe** (60%) and **Spamming** (57%). Etwa die Hälfte der Befragten zeigte sich besorgt über die Möglichkeit, im Internet zufällig auf **kinderpornografisches Material** (52%) oder **Hassrede** zu stoßen (46%).

Trotz dieser Bedenken gaben etwa 74% an, **sich selbst vor Cyberkriminalität schützen zu können**.

[75] Eine Firewall ist eine Software und/oder Hardware, die den Computer und das Netzwerk vor unerlaubtem Zugriff schützen soll.

4.2. Von den Folgen zu den Bedürfnissen der Opfer von Cyberkriminalität

Allgemein ähneln die Bedürfnisse eines Cyberkriminalitätsopfers denen der Opfer *herkömmlicher* Formen der Kriminalität und es können verschiedene Arten von Bedürfnissen festgestellt werden (Leukfeldt et al., 2020).

Während die Bedürfnisse, die mehr oder weniger allen Opfern jeglicher Form von Kriminalität gemein sind, aufgelistet werden können, gibt es besondere Bedürfnisse, die sich abhängig von der Art der Viktimisierung und dem zeitlichen Rahmen unterscheiden (d. h. die Bedürfnisse eines Cyberkriminalitätsopfer direkt nach dem Verbrechen werden von denen unterschieden, die einzige Zeit nach dem Verbrechen auftreten).

Zudem hängen die Bedürfnisse eines Kriminalitätsopfers auch von dessen persönlichen Merkmalen, sozialem Umfeld und den Konsequenzen der einzelnen Tat ab (Huang, 2018, Wood et al., 2015 *cit in idem*).

Die folgende Tabelle fasst die Bedürfnisse zusammen, die bei Cyberkriminalitätsopfern festgestellt und durch die Cyber-Viktimisierungserfahrung verursacht wurden (Cross et al., 2016; Leukfeldt et al., 2020). Der Inhalt der Tabelle ist aufgrund der mangelnden Forschung zum Thema nicht vollständig.

Tabelle 3: Bedürfnisse von Cyberkriminalitätsopfern

Emotionale und psychologische Bedürfnisse	Verfahrens- und informationsrelevante Bedürfnisse	Praktische und finanzielle Bedürfnisse
• Anerkennung als Kriminalitätsopfer • Anerkennung der Cyber-Viktimisierungserfahrung • Bedürfnis, mit jemandem über die Erfahrung zu sprechen, der oder die zuhört • Anerkennung der Cyber-Viktimisierungserfahrung von außen (informeller gesellschaftlicher Kontext und Behörden) • Qualifizierte und vertrauliche Unterstützung nach der Erfahrung mit Cyberkriminalität • Erholung von den emotionalen und psychologischen Folgen von Cyberkriminalität • Zugang zu professionel-ler/qualifizierter Unterstützung	• Informationen über bestehende Hilfsangebote/-strukturen und wie man diese erreicht • Unterstützung bei der Meldung der Straftat und dem Erstatten der Anzeige • Informationen über den Täter, die Untersuchung und das Gerichtsverfahren • Informationen über das Ergebnis des Strafverfahrens • Entschädigung für die Tat	• Hilfe beim Entfernen der cyberkriminellen Inhalte aus dem Internet und IKT • Unterstützung bei der Kontaktaufnahme zu Banken, Internetdienstanbietern und anderen Plattformen • Hilfe bei der Wiederherstelung eines Sicherheitsgefühls (Erhalt physischer Integrität) und Verhinderung erneuter Viktimisierung • Schutz vor dem Täter • Finanzielle Verluste durch den Verlust von Vermögenswerten/Informationen • Finanzielle Entschädigung für Verluste durch Cyberkriminalität

Die Art und Weise, wie die Einrichtungen verschiedenster Systeme und Strukturen, wie dem Justiz- oder Gesundheitssystems, dem System der sozialen Absicherung oder ziviler Organisationen, angesichts der Bedürfnisse der Kriminalitätsopfer und besonders im Hinblick auf die Bedürfnisse

der Cyberkriminalitätsopfer tätig werden, kann zu einer **sekundären Viktimisierung** führen. Dabei handelt es sich um eine zweite Form der Viktimisierung, die durch unzureichende Unterstützung dieser Systeme und Strukturen und die Diskrepanz zwischen dieser Unterstützung und den Interessen, Bedürfnissen und Rechten der Opfer entsteht.

HIGHLIGHT | ANGEBOTE IM FOKUS:

Im Hinblick auf institutionsübergreifende Zusammenarbeit unterstützt WePROTECT Global Alliance eine koordinierte Maßnahme gegen sexuelle Ausbeutung und Missbrauch von Kindern im Internet auf nationaler Ebene.

Das vorgeschlagene Modell berücksichtigt die Tatsache, dass sexuelle Ausbeutung und Missbrauch von Kindern im Internet nicht isoliert bekämpft werden kann, sondern eine breitere Auswahl an Maßnahmen zur Prävention und Bekämpfung erfordert, um eine umfassende Strategie auf nationaler Ebene zu realisieren.

Die Probleme der verschiedenen Systeme/Dienste und institutioneller Strukturen bei der Reaktion auf die Bedürfnisse von Cyberkriminalitätsopfern (*idem*) könnten ihre Ursache in den folgenden Einschränkungen haben:

- Unzureichende menschliche und materielle Ressourcen;
- Ignoranz gegenüber den Bedürfnissen und Rechten des Opfers oder Probleme bei deren Umsetzung;
- Notwendigkeit besonderer Ausbildung/Kenntnisse für Kontaktaufnahme und Umgang mit Cyberkriminalitätsopfern;
- Schwierigkeiten mit dem Ablauf des Strafverfahrens, einschließlich der Identifizierung eines Verdächtigen, dem Erstatten einer Anzeige, der Untersuchung und Strafverfolgung.

4.3. Finanzielle und wirtschaftliche Kosten durch Cyberkriminalität

Cyberkriminalität verursacht verschiedenen Entitäten hohe Kosten, besonders wenn kollektive Entitäten das Ziel sind. Das Ausmaß der wirtschaftlichen und finanziellen Schäden durch Cyberkriminalität variiert abhängig von der Branche, der Größe der Organisation, den Daten und der Schwere der Form(en) von Cyberkriminalität, die zur Anwendung kommt (Gañán, Ciere & van Eeten, 2017).

Cyberkriminalität, die sich gegen kollektive Entitäten wie Unternehmen und Organisationen richtet, zielt in der Regel und besonders bei größeren Entitäten auf Zugriff auf deren Datenressourcen ab. Kleinere Entitäten scheinen andererseits weniger attraktive Ziele für Cyberkriminalität darzustellen (Gañán et al., 2017).

Die wirtschaftlichen und finanziellen Kosten für Entitäten durch Cyberkriminalität sind häufig nicht

der tatsächliche Verlust von Geld, sondern **immaterielle Effekte**. Die Frage nach einer realistischen, monetären Kosteneinschätzung mag verständlich sein, ist aber schwierig zu messen, da nur einige der wirtschaftlichen und finanziellen Folgen von Cyberkriminalität mithilfe empirischer Daten in Geldbeträge umgerechnet werden können, viele aber nicht (*idem*).

Die Kosten, die durch Cyberkriminalität entstehen, lassen sich einteilen in die Kosten in Erwartung der Cyberkriminalität, als Folge der Cyberkriminalität und als Reaktion auf Cyberkriminalität (*idem*).

Die Kosten in Erwartung und als Folge der Cyberkriminalität beinhalten die Kosten (vorher und/oder nachher) für die **Risikoeinschätzung**, den Aufbau von **Cybersicherheitsmaßnahmen** und die Anschaffung von **Schutzmaßnahmen wie Software und Hardware**. Diese Kosten können auch fachliche Beratung über Cybersicherheit und das Testen, Überwachen und regelmäßige Aktualisieren der Sicherheitsrisiken, Verfahren und Systeme beinhalten (Das & Nayak, 2013).

Die Kosten als Reaktion auf Cyberkriminalität umfassen alle **Ausgaben und Maßnahmen des öffentlichen oder privaten Sektors im Kampf gegen Cyberkriminalität**, die auch von der Gesellschaft getragen werden, einschließlich der Kosten für das Justizsystem, das Cyberkriminalität untersucht und verfolgt (Gañán et al., 2017).

HIGHLIGHT | WICHTIGSTE INFORMATION:

Einfluss von Cyberkriminalität auf das Vertrauen der Nutzer

Es entstehen im Voraus Kosten, um das Vertrauen der Nutzer und Verbraucher in die Sicherheit im Internet und in IKT sicherzustellen.

Verbraucher ziehen E-Commerce und Online-Aktivitäten dem Einkauf in beispielsweise Geschäften vor, da der Konsum und Kauf von Artikeln, Produkten und Dienstleistungen über das Internet und IKT als bequem, leicht zugänglich und sicher gelten.

Cyberkriminalität untergräbt die scheinbaren Vorteile der Internet- und IKT-Nutzung und erhöht **Risikowahrnehmungsindizes** der Nutzer und Verbraucher im Internet, während gleichzeitig das Vertrauen nachlässt. So verändert Cyberkriminalität die Einstellung zum Konsum von Online-Inhalten.

Wenn die Risikowahrnehmung im Hinblick auf Cyberkriminalität das Vertrauen der Nutzer oder Verbraucher in die Verwendung des Internets oder IKT für bestimmte Aktivitäten untergräbt, nimmt die Attraktivität der Onlineplattformen für den Konsum oder Kauf der Artikel, Produkte oder Dienstleistungen ab, was wiederum Onlinegewohnheiten und -verhalten verändern kann (Saban, McGivern & Saykiewicz, 2002; Smith, 2004; Saini, Rao & Panda, 2012).

TEIL II
INTERVENTION

TEIL II

INTERVENTION

1. DIE ROLLE DER FACHKRAFT BEI DER BETREUUNG VON CYBERKRIMINALITÄTSOPFERN

Dieses Kapitel widmet sich der Bedeutung und der Rolle der Fachkräfte, die Cyberkriminalitätsopfer betreuen und den dafür notwendigen Kompetenzen. Wir gehen außerdem auf die psychosozialen Risiken ein, die aus dem Umgang mit Kriminalitätsopfern im Allgemeinen und Cyberkriminalitätsopfern im Besonderen erwachsen.

1.1. Persönliche Voraussetzungen

Die Betreuung von Kriminalitätsopfern, besonders in Fällen von Cyberkriminalität, erfordert einige wichtige Fähigkeiten.

Persönliche Voraussetzungen umfassen die Persönlichkeit und Persönlichkeitsmerkmale einer Betreuungskraft und inwiefern diese zur Tätigkeit und dem Aufgabenfeld passen. Sie sind in jedem Pflege- oder Betreuungsberuf unabdingbar und besonders für Fachkräfte im Bereich Krisenintervention von essenzieller Wichtigkeit (APAV, 2013b), zum Beispiel bei der Betreuung von Cyberkriminalitätsopfern.

Die fachlichen Hauptkompetenzen für die Betreuung und den Umgang mit Kriminalitätsopfern, wie Empathie, Offenheit und Verfügbarkeit, werden im Folgenden dargelegt (Pessoa, from Mota Matos, Amado & Jäger, 2011).

Außerdem sollte **die Fachkraft in der Lage sein**, bei der Betreuung von Kriminalitätsopfern **positive zwischenmenschliche Beziehungen aufzubauen und aufrechtzuerhalten**. Das schließt Kontakt und Interaktion mit Opfern, ihren Verwandten und Freunden sowie anderen Fachkräften und Partnerorganisationen ein, die in diesem Bereich tätig sind. Diese Beziehungsdimension – das Kümmern um zwischenmenschliche Beziehungen – schließt die Fähigkeit zur **friedlichen Beilegung zwischenmenschlicher und/oder institutioneller Konflikte sowie positiven Stressmanagements** ein. Diese sind gute Indikatoren für die Fähigkeit, sich auf andere einzulassen, besonders in einem so komplexen und fordernden Kontext, in dem die Fachkraft unter Umständen permanent mit Menschen in Not konfrontiert ist (APAV, 2013b; APAV, 2017).

Emotionales Selbstmanagement gehört ebenfalls zu den Schlüsselkompetenzen – die Fähigkeit, seine eigenen Emotionen in stressigen, frustrierenden und herausfordernden Situationen zu kontrollieren (APAV, 2013b). Kontakt und Interaktion mit Kriminalitätsopfern erfordert ein hohes Maß an emotionaler Belastbarkeit, um einerseits auf die Gewalt- oder Kriminalitätserfahrungen der Opfer eingehen zu können und ihnen Unterstützung anbieten zu können (und mit dem Stress und der Frustration jedes Falls umgehen zu können) und andererseits den Einfluss auf die emotionale Ausgeglichenheit der Fachkraft verkraften zu können (APAV, 2017).

Die Fachkraft sollte ebenfalls über **Toleranz und Respekt gegenüber kulturellen Werten und Unterschieden** verfügen: Sie muss unabhängig von den Einstellungen oder Merkmalen des Opfers stets offen und positiv sein. Neutralität und Objektivität bilden die Grundlage für effektive Betreuung

und Fachkräfte sollten ihre persönlichen Werte und Glaubensgrundsätze kontrolliert zurückstellen, wenn sie ein Opfer betreuen (*idem*). Die Basis jeder Betreuung von Kriminalitätsopfern ist der **Respekt vor der Menschenwürde**. Das Opfer muss bedingungslos als Mensch angesehen werden, ebenso wie die Fachkraft selbst, aber ohne deren Einzigartigkeit und Individualität zu vergessen.

Zwei grundlegende Prinzipien bei der Kontaktaufnahme zu und der Betreuung von Kriminalitätsopfern sind:

- **Mitgefühl und Empathie:**

  Die Fähigkeit, sich in *eine andere Person oder deren Lage hineinzuversetzen* ist bei der Kontaktaufnahme zu und der Betreuung und Unterstützung eines Kriminalitätsopfers unverzichtbar. Die Fähigkeit, die Dinge aus der Perspektive des Opfers zu sehen, und ein gewisses Einfühlungsvermögen für die Erfahrung des Opfers sowie die Gefühle und Reaktion des Opfers auf die Straftat erkennen und verstehen zu können spielt eine wichtige Rolle beim Aufbau einer **unterstützenden und vertrauensvollen Beziehung zwischen Fachkraft und Opfer** und kann ausschlaggeben für den Erfolg der Betreuungs- und/oder Unterstützungsmaßnahme sein.

  Empathie bedeutet nicht, dass die Fachkraft emotional auf die Beschreibungen des Verbrechens durch das Opfer reagieren soll; entscheidend ist dagegen die Fähigkeit der Fachkraft, seine/ihre Emotionen auf gesunde Weise zu kontrollieren. Diese Ausgeglichenheit ist von größter Wichtigkeit, da sie dem Kriminalitätsopfer dabei hilft, die Fachkraft als emotionalen Ankerpunkt zu sehen, als jemanden, der mit der Situation umgehen kann und für seine Aufgabe qualifiziert ist (APAV, 2017; APAV 2019).

- **Begabung:**

  Dabei handelt es sich mehr um eine persönliche Voraussetzung als um eine erlernbare Fähigkeit – die natürliche Verinnerlichung sozialer Solidarität spielt eine wichtige Rolle im Umgang mit Kriminalitätsopfern und bei ihrer Unterstützung, Aufklärung und der Durchführung von Hilfsmaßnahmen (APAV, 2017).

1.2. Wichtigste und zusätzliche Qualifikationen

Zusätzlich zu den o. g. persönlichen Voraussetzungen muss die Fachkraft, die Kriminalitätsopfer im Allgemeinen und Cyberkriminalitätsopfer im Besonderen kontaktiert und betreut über eine entsprechende Ausbildung verfügen. Des Weiteren sollte die Fachkraft bei einer Institution tätig sein, egal ob diese öffentlich, privat, staatlich oder nichtstaatlich ist oder auf ehrenamtlichem Engagement aufgebaut ist (APAV, 2013b).

Eine Ausbildung (d. h. ein akademischer Abschluss) in einer anerkannten Disziplin (wie zum Beispiel Sozialwissenschaften oder einem anderen Bereich, abhängig von der Art der Betreuung, die die

Fachkraft und/oder Hilfsorganisation anbietet) und eine gewisse **Berufserfahrung** sind wichtige Voraussetzung für die Betreuung von Kriminalitätsopfern, einschließlich der Opfer der verschiedenen Formen der Cyberkriminalität (APAV, 2017).

Einige Fachkräfte sind, abhängig von den festgestellten Bedürfnissen des Opfers und der Art der angeforderten Unterstützung, besser geeignet, auf die Interessen, individuellen Bedürfnisse und Rechte der verschiedenen Kriminalitätsopfer einzugehen. Es versteht sich von selbst, dass zum Beispiel rechtliche Beratung durch eine Fachkraft mit juristischer Ausbildung und psychologische Unterstützung durch ausgebildete Psychologen erfolgen muss[76].

Angesichts der Vielfalt der Bedürfnisse und Konsequenzen, mit denen Cyberkriminalitätsopfer[77] konfrontiert sind, ist **interdisziplinäre Unterstützung und Betreuung** erforderlich. Diese können den Einsatz von Fachkräften mit verschiedenen Ausbildungen, aber auch die Einbeziehung verschiedener Organisationen erfordern. Ein Netzwerk aus Fachkräften mehrerer Bereiche und Organisationen mit unterschiedlichen Schwerpunkten, Erfahrungen und aus verschiedenen Betreuungsphasen trägt zu einer verbesserten Betreuung eines jeden Cyberkriminalitätsopfers bei.

Zusätzlich zu einer akademischen Ausbildung und relevanter Berufserfahrung sollte eine Fachkraft, die Cyberkriminalitätsopfer kontaktiert oder betreut, regelmäßig und fortlaufend an **spezifischen Trainingsmaßnahmen** für den Umgang mit Kriminalitäts- und Cyberkriminalitätsopfern und über das Forschungsgebiet der Cyberkriminalität teilnehmen (APAV, 2013b; APAV, 2017). In diesen spezifischen Trainingsmaßnahmen sollten u. a. die folgenden Inhalte behandelt werden: theoretisches, kriminologisches und viktimologisches Verständnis der verschiedenen Formen der Cyberkriminalität; Kenntnis über die Folgen, Auswirkungen und Dynamik der Cyberkriminalität sowie über die Bedürfnisse und Rechte der Opfer; juristische Rahmenbedingungen und existierende rechtliche und gesellschaftliche Reaktionen; Cybersicherheit.

Angesichts der Natur der Cyberkriminalität und der Technologie, gegen die sie sich richtet (oder mithilfe derer sie verübt wird), erfordert der Kontakt zu und die Betreuung von Cyberkriminalitätsopfern außerdem **Kompetenz und spezifisches Training im Umgang mit dem Internet, IKT und anderer Technologien**, und zwar sowohl im Hinblick auf deren Funktionsweise und die Kommunikationswerkzeuge, die durch das Internet beeinflusst werden (einschließlich sozialer Netzwerke), als auch hinsichtlich der Frage, wie diese für die Verübung von Straftaten eingesetzt und/oder selbst zum Ziel von Cyberkriminalität werden können (Bloom, 2007, Poh et al., 2013, Trepal et al., 2007, Mallen, Vogel, & Rochlen, 2005 cit *in* APAV, 2017). Die **Informations- und Technikkompetenz** der Fachkraft ist maßgeblich für ihre Fähigkeit, die beständige Weiterentwicklung der IKT, die Kommunikationstrends im Internet und die permanente und konsequente Evolution der Cyberkriminalität im Blick zu behalten.

Nicht weniger wichtig sind **Kommunikationsfähigkeite**n bei der Kontaktaufnahme oder Betreuung von Cyberkriminalitätsopfern, wie aktives Zuhören, aber auch die Formulierung klarer, verständlicher Botschaften in komplexen Kontexten als Teil des Unterstützungsprozesses (Person et al., 2011). Das

[76] Siehe Teil II, Kapitel 3, Abschnitt 3.5 dieses Handbuchs für Informationen über die Schlüsselaspekte der fachlichen Beratung für Cyberkriminalitätsopfer.

[77] Siehe Teil I, Kapitel 4 dieses Handbuchs für weitere Informationen zum Thema.

folgende Kapitel dieses Handbuchs behandelt Kommunikation und Empathie als die Grundlagen des Betreuungsprozesses und der Beziehung zwischen Fachkräften und Cyberkriminalitätsopfern ausführlicher.

1.3. Psychosoziale Risiken durch Kontakt und Betreuung von Cyberkriminalitätsopfern

Fachkräfte, die in engem Kontakt zu Kriminalitätsopfern stehen, leiden häufig an **körperlicher und geistiger Erschöpfung, psychischer Belastung und berufsbedingtem Stress**, da sie aufgrund ihrer Funktion in direktem Kontakt mit Personen in (emotional wie körperlich) besonders anfällige und fragilen Situationen kommen, die durch Viktimisierung und Cyber-Viktimisierung entstanden sind. Die Fachkräfte sehen sich nicht nur mit den persönlichen Viktimisierungserfahrungen anderer Personen konfrontiert, sondern auch mit der Frustration über die Diskrepanz zwischen den Erwartungen und Bedürfnissen des Opfers und dem, was mit den vom System und institutionellen Strukturen bereitgestellten Ressourcen möglich ist. Zusätzlich zu der im Rahmen der Betreuung *normalen* Berührung mit den persönlichen Viktimisierungserfahrungen des Opfers (die Wichtigkeit, Informationen zu sammeln wird in den folgenden Kapiteln dieses Handbuchs dargelegt) müssen Fachkräfte u. U. bestimmte Inhalte wie Bilder, Fotos und/oder Videos krimineller Herkunft ansehen, die bei der Art von Cyberkriminalität entstanden sind, die gegen das betreute Opfer begangen wurde, was eine weitere potenzielle Stresssituation oder sogar traumatische Situation für die Fachkraft sein kann. Die Inhalte können sehr gewalttätiger oder sogar explizit sexueller Natur sein, zum Beispiel wenn Kinder und Heranwachsende betreut werden, die Opfer sexuellen Missbrauchs und/oder sexueller Ausbeutung über das Internet geworden sind, oder bei der Betreuung von Cyberstalking-Opfern, Opfern von Erpressung mit sexuellen Inhalten oder Opfern von nichteinvernehmlicher Verbreitung von Bildern und Videos, z. B. Rachepornos[78]. Der fortlaufende Kontakt mit dieser Art potenziell traumatischer Inhalte kann das Wohlbefinden und die geistige Gesundheit der betreuenden Fachkraft beeinträchtigen (McCann & Pearlman, 1990).

Daher tritt nicht selten das Burnout-Syndrom auf, kurz definiert als ein Syndrom (oder eine Reihe von Symptomen), einschließlich **emotionaler Erschöpfung, Depersonalisation**[79] und **ein niedriges Maß an Erfüllung eigener Bedürfnisse** als Reaktion auf stressige Arbeitsbedingungen (Campos, Jordani, Zucoloto, Bonafé & Maroco, 2012).

Die folgende Tabelle fasst einige präventive organisatorische Maßnahmen und individuelle Verhaltensweisen für den Kontakt mit oder die Betreuung von Cyberkriminalitätsopfern zusammen, die psychosoziale Risiken verhindern sollen, die bei der Betreuung von Kriminalitäts- und Cyberkriminalitätsopfern auftreten.

[78] Detaillierte Informationen über diese Formen der Cyberkriminalität finden Sie in Teil I, Kapitel 1 dieses Handbuchs.

[79] Depersonalisation ist der Prozess der Entmenschlichung bei der Behandlung/dem Kontakt mit anderen, der sich durch zwischenmenschliche Interaktion ohne Affektivität und Empathie auszeichnet.

Tabelle 1: Maßnahmen gegen psychosoziale Risiken, die bei der Betreuung von Kriminalitäts- und Cyberkriminalitätsopfern auftreten

Organisatorische Maßnahmen des Dienstanbieters	Individuelle Verhaltensweisen der Fachkraft
• Förderung einer Unternehmenskultur, die offen für Feedback und das Teilen von Erfahrungen ist • Bereitstellung interner und/oder externer psychologischer Beratungs- oder Hilfsangebote für die Fachkräfte • Einrichtung von Beratungsstellen (einzeln oder in der Gruppe), die das Wohlbefinden der Beratungsfachkräfte fördern • Regelmäßige Besprechungen über die Erfahrungen/ Fälle mit Gleichgestellten, dem Team oder anderen Betreuungsfachkräften • Bereitstellung der erforderlichen Ausrüstung, logistischen Ressourcen und Maßnahmen für die Förderung des Wohlbefindens am Arbeitsplatz • Förderung von Freizeit- und Erholungsaktivitäten, die nicht in Verbindung mit den beruflichen Aufgaben und Funktionen stehen	**Selbstfürsorge:** • Sport • Freizeitaktivitäten • Einhaltung grundlegender gesundheitsfördernder Maßnahmen, ausgewogene Ernährung und ausreichend Schlaf • Kontakt zu Familie und Freunden • Bewusstsein und Anerkennung der Grenzen von Körper und Geist • Sicherstellung ausreichender Ruhephasen ohne Kontakt zur Arbeit, idealerweise während Aktivitäten, die Freude machen • Anwendung von Entspannungs- und Meditationstechniken • Zeit in der Natur **Weiterführende Maßnahmen:** • Zugang zu psychologischer Beratung über den Arbeitgeber, entweder intern oder extern • Teilnahme an individueller oder Gruppenberatung (Teams/Paare)

2. WICHTIGE ASPEKTE FÜR DEN ERSTEN KONTAKT ZU CYBERKRIMINA-LITÄTSOPFERN

Dieses Kapitel beinhaltet einige grundlegende Richtlinien für den ersten Kontakt zu Cyberkriminalitätsopfern und die Schritte, die erforderlich sind, bevor tiefergehende und qualitativere Maßnahmen ergriffen werden können, die von jeder Hilfsorganisation für Cyberkriminalitätsopfer eingehalten werden sollten.

Zu diesem Zweck arbeiten wir die Hauptgrundlagen für den Aufbau einer Vertrauensbeziehung zwischen Opfer und Betreuungsfachkraft heraus, einschließlich Kommunikation und Empathie, aber auch hinsichtlich des Sammelns von Informationen und wie dieses jeden weiteren Kontakt zum Opfer beeinflusst. Dieses Kapitel endet mit einem Ansatz für die Betreuung von Cyberkriminalitätsopfern im Kindes- und Heranwachsendenalter unter Berücksichtigung ihres besonderen Schutzbedürfnisses.

2.1. Allgemeine Richtlinien für den ersten Kontakt mit Cyberkriminalitätsopfern

Für das Opfer von Cyberkriminalität ist die Suche nach Hilfe ein wichtiger und maßgeblicher Schritt im emotionalen und psychischen Heilungsprozess und auf dem Weg zur Wiederherstellung der Normalität in seinem oder ihrem Leben.

Wie die Opfer herkömmlicher Straftaten sucht sich auch nur ein kleiner, nicht bestimmbarer Anteil der Cyberkriminalitätsopfer professionelle Hilfe, besonders bei Opferberatungs- und Hilfseinrichtungen. Obwohl häufig keine Unterstützung in Anspruch genommen wird (Cross et al., 2016), aus Gründen, die denen für die Nicht-Anzeige von Cyberkriminalität ähneln[80], gilt allgemein, dass die Suche nach Hilfe von zwei Faktoren abhängt: Das Opfer erkennt sich selbst als Opfer einer Straftat an und stuft das Cyber-Verbrechen als schwerwiegend ein (De Kimpe et al., 2020).

Im Folgenden stellen wir einige allgemein gültige Richtlinien für Fachkräfte vor, die Opfer von Straftaten, einschließlich Cyberkriminalität, betreuen (Winkel, 1991; Machado & Gonçalves, 2003 cit *in APAV*, 2013b; Cross, Richards & Smith, 2016; Wedlock & Tapley, 2016; De Kimpe, Ponnet, Walrave, Snaphaan, Pauwels & Hardyns, 2020).

[80] Siehe Teil I, Kapitel 1, Abschnitt 1.4 dieses Handbuchs für weitere Informationen über die Diskrepanz zwischen angezeigten Cyber-Verbrechen und den tatsächlich begangenen.

Tabelle 2: Allgemeine Richtlinien für den ersten Kontakt mit Cyberkriminalitätsopfern

Ziele	Maßnahmen
Anerkennung für die Meldung/ Anzeige	Den Mut anerkennen, den das Opfer aufbringen musste, um sich Hilfe zu suchen und über die persönliche Cyber-Viktimisierungserfahrung zu sprechen.
Einlassen auf die Geschwindigkeit des Opfers und Bestärkung beim Teilen der Erfahrung	Stellen offener Fragen wie „Was möchten Sie uns erzählen?“, die eine sichere Atmosphäre für das Teilen von Informationen schaffen. Respekt und Förderung emotionaler Aussprache und Momenten großer Fragilität und Emotionalität, die beim Sprechen über die Erfahrung mit Cyberkriminalität auftreten können. Ohne Druck nachfragen, wenn die Informationen unklar oder unvollständig sind. Zeitlichen Ablauf, Pausen und Schweigen des Opfers, einschließlich Zögern bei der Weitergabe von Informationen, akzeptieren.
Anerkennung der Erfahrung	Einfühlsames und aktives Zuhören, Wertschätzung der Reaktionen, Emotionen, Verhaltensweisen, Gedanken und Bedeutung, die das Opfer seiner oder ihrer Viktimisierungs- bzw. Cyber-Viktimisierungserfahrung zuschreibt. Zeigen Sie dem Opfer, dass Sie seinen oder ihren Erzählungen Glauben schenken, ohne zu verurteilen. Normalisieren Sie die Reaktion des Opfers.
Wiedererlangung der Kontrolle	Bereitstellung eindeutiger Informationen mit dem Fokus auf die Informationen darüber, was passiert ist, und welche Schritte als nächstes erfolgen werden, in einfachen, klaren Worten unter Berücksichtigung der persönlichen Merkmale des Opfers. Treffen Sie keine Entscheidungen für das Opfer, akzeptieren Sie die Entscheidungen des Opfers, ohne zu urteilen und unterstützen sie deren Umsetzung, sodass das Opfer die Kontrolle über sein oder ihr Leben zurückerlangen kann. Respektieren Sie die Entscheidungen des Opfers.
Das Opfer ist kein „Einzelfall“	Informieren Sie das Opfer über das Verbrechen und seine Häufigkeit.
Keine Schuldzuweisungen	Kritisieren Sie nicht. Ordnen Sie die Reaktionen des Opfers in den emotionalen Kontext eines solchen Verbrechens ein. Würdigen Sie vorangegangene Versuche des Opfers, sich zu schützen, auch wenn diese nicht erfolgreich waren. Vermeiden Sie Formulierungen wie „Warum haben Sie nicht …“ und „Sie hätten besser …“.
Verhindern Sie Rückzug und Isolation	Empfehlen Sie die schrittweise Wiederaufnahme von Aktivitäten, einschließlich Internet- und IKT-Nutzung. Fördern Sie die Wiederaufnahme von Aktivitäten, die dem Opfer vor der Tat Spaß gemacht haben, besonders offline. Sorgen Sie für sozialen Halt. Vermeiden Sie Überfürsorglichkeit durch Familie und Freunde (ohne die Sicherheit des Opfers zu vernachlässigen).
Fördern Sie die emotionale und kognitive Verarbeitung der Erfahrung	Weisen Sie das Opfer auf keinen Fall an, „alles zu vergessen“ und halten Sie die Personen in seinem oder ihrem engeren Umfeld ebenfalls an, das nicht zu tun. Schlagen Sie dem Opfer vor, mit Vertrauenspersonen über seine oder ihre Gefühle und Ängste zu sprechen und bitten Sie diese Personen, verfügbar zu sein, ohne das Opfer unter Druck zu setzen.
Verhindern Sie weitere Verbrechen	Besprechen Sie Sicherheits- und Cybersicherheitsmaßnahmen. Schärfen Sie das Bewusstsein für die Risiken der Internet- und IKT-Nutzung und empfehlen Sie die Einrichtung von Cybersicherheitsmechanismen und persönlicher Schutzmaßnahmen bei der Verwendung des Internets oder IKT. Falls nötig, erstellen Sie mit dem Opfer einen Sicherheitsplan (besonders wenn neben der Cyber-Viktimisierung auch eine Viktimisierung im *herkömmlichen* Sinn stattfand).
Beziehen Sie Vertrauenspersonen in den Heilungsprozess mit ein	Sofern das Opfer einwilligt, sollten Sie die Familie und/oder Freunde in den Heilungsprozess miteinbeziehen und sie um Unterstützung bei der Verarbeitung der Erfahrung und Verhinderung von weiteren Verbrechen, Rückzug und Isolation.

2. WICHTIGE ASPEKTE FÜR DEN ERSTEN KONTAKT ZU CYBERKRIMINA-LITÄTSOPFERN

Des Weiteren stellen wir im Folgenden eine Reihe bewährter Methoden und häufiger Fehler im Umgang mit Kriminalitätsopfern vor (APAV, 2019b).

Tabelle 3: Bewährte Methoden vs Fehler im Umgang mit Cyberkriminalitätsopfern

Bewährte Methoden im Umgang mit Cyberkriminalitätsopfern	Fehler im Umgang mit Cyberkriminalitätsopfern
Der Aussage des Opfers glauben.	Der Aussage des Opfers keinen Glauben schenken.
Das Opfer ermutigen, über seine oder ihre Cyber-Viktimisierungserfahrung zu sprechen, ohne Druck auszuüben.	Übernahme des Entscheidungsprozesses des Opfers. Dieser Fehler ist an Formulierungen wie „Sie sollten nicht …“ oder „Sie müssen …“ zu erkennen.
Vertraulichkeit und ihre Grenzen akzeptieren. Nicht verurteilen.	Entscheidungen, ohne die vorherige Einwilligung des Opfers zu treffen.
Die Wahrnehmung des Opfers bezüglich seiner oder ihrer Situation respektieren, auch wenn diese sich von der einer Fachkraft unterscheidet.	Dem Opfer ein falsches Sicherheitsgefühl zu vermitteln, unrealistische Erwartungen an die Rolle der Fachkraft, Lösung der Situation oder Bedürfnisse des Opfers zu fördern, erkennbar an Formulierungen wie „Machen Sie sich keine Sorgen. Alles wird gut.“
Cyber-Viktimisierungserfahrung und die damit zusammenhängenden Reaktionen, Emotionen und Gedanken normalisieren.	Verharmlosung des Problems und seiner Auswirkungen.
Dem Opfer erklären, dass andere Personen ähnliche Situationen erleben und er oder sie kein „Einzelfall“ ist.	Überfürsorge gegenüber dem Opfer.
Dem Opfer begreiflich machen, dass er oder sie nicht für die Situation verantwortlich ist und beim Umgang mit Schuldgefühlen unterstützen.	Unangemessen starkes Interesse an Details der Cyber-Viktimisierung, über die das Opfer nicht sprechen will (oder noch nicht sprechen kann).
Dem Opfer beim Entscheidungsprozess helfen, indem die Vor- und Nachteile aller Optionen aufgezeigt werden, damit fundierte Entscheidungen getroffen werden können.	Wenig Zeit oder Verfügbarkeit für das Opfer und um ihm oder ihr zuzuhören, zum Beispiel durch körperliche Anzeichen von Rastlosigkeit und/oder Unterbrechung seiner oder ihrer Schilderungen.
Beurteilung des Risikos einer (erneuten) Cyber-Viktimisierung und der Bedürfnisse des Opfers, Bereitstellung angemessener Hilfe in Abhängigkeit der Situation des Opfers und/oder Weiterempfehlung an Hilfsdienste oder -organisationen.	Deutung oder Diagnose der Reaktionen, Gefühle und Gedanken des Opfers bezüglich seiner oder ihrer Cyber-Viktimisierungserfahrung, die sich in Formulierungen wie „Sie tun das, weil …“ äußern.
Bereitschaft, in Krisensituation einzugreifen.	Anbieten von Lösungen, ohne das Opfer in den Entscheidungsprozess miteinzubeziehen.
	Unangemessener Humor oder unnötige Enthüllungen über die eigene Person als Strategien, eine Vertrauensbeziehung aufzubauen.

2.2. Die Wichtigkeit von Kommunikation und Empathie

Empathie zeichnet sich, wie oben erwähnt, durch die Fähigkeit aus, die Perspektive einer anderen Person zu verstehen und deren momentane Gefühle, ihre Gefühle während der Cyber-

Viktimisierungserfahrung und hinsichtlich der Tat zu erkennen und zu begreifen sowie Verständnis zu zeigen und Reaktionen wie Unbehagen, Besorgnis oder andere als mehr oder weniger sofortige Auswirkung der Cyberkriminalität zu akzeptieren.

Die Empathie der Fachkraft gegenüber dem Opfer und seiner oder ihrer Cyber-Viktimisierungserfahrung ist sehr wichtig für den **Aufbau einer vertrauensvollen und unterstützenden Beziehung zwischen der Fachkraft und dem Opfer** und ausschlaggebend für die Umsetzung der o. g. Ziele (siehe Tabelle 2).

Empathie spielt eine **tragende Rolle in der menschlichen Kommunikation**, da sie den Kommunikationsprozess vereinfacht und das Opfer dazu ermutigt, über seine oder ihre Erfahrung zu sprechen, einschließlich Informationen und Beweise, die zum Erfolg der Betreuung, des Heilprozesses des Opfers und der Erfüllung seiner oder ihrer Bedürfnisse, aber auch des strafrechtlichen Verfahrens beitragen (De Vignemont & Singer, 2006; Sommers-Flanagan & Sommers-Flanagan, 2014, Themeli, 2014, Morrison, 2014 cit in APAV, 2018).

HIGHLIGHT | WICHTIGSTE INFORMATION:

Empathie darf nicht bedeuten, dass die Fachkraft die Kontrolle über sich verliert und zusammen mit dem Opfer weint. Ein solches Verhalten kann, auch unbeabsichtigt, negative Auswirkungen auf das Opfer und auf die Qualität der Betreuung haben, da das Opfer die Fachkraft u. U. nicht länger als qualifizierte Unterstützung wahrnehmen kann.

Folgende Aspekte sollte die Fachkraft bei **empathischer Kommunikation** berücksichtigen (APAV, 2019b):

- Halten Sie ruhigen, unaufdringlichen Augenkontakt mit dem Opfer.
- Sprechen Sie während des Augenkontakts mit klarer, interessierter Stimme und zeigen Sie mit Ihrer Körpersprache Verfügbarkeit und Ruhe (Sehen Sie zum Beispiel nicht auf die Uhr, zeigen Sie keine Anzeichen von Ungeduld und unterbrechen Sie das Opfer nicht unnötig).
- Verwenden Sie Einwürfe, um das Opfer in seiner oder ihrer Entscheidung, über die Cyber-Viktimisierungserfahrung zu sprechen und Hilfe zu suchen, bestärken.
- Zeigen Sie deutlich, dass Sie dem Opfer aufmerksam zuhören (z. B. durch bestätigendes Nicken).
- Stellen Sie sicher, dass Sie die Informationen, die Ihnen das Opfer gibt, richtig verstehen, zum Beispiel durch:

    - Umformulierung – Wiederholen Sie das Gesagte in Ihren eigenen Worten. Die Verwendung eigener Worte hilft der Fachkraft dabei sicherzustellen, dass er oder sie das Opfer richtig verstanden hat, vermittelt dem Opfer aber auch indirekt, dass man ihm genau zuhört, was ihn oder sie zum Weitermachen ermutigen wird.
    - Zusammenfassung – Fassen Sie die Informationen des Opfers zusammen, wenn Sie ein Thema abschließen, am Ende einer Sitzung und/oder zu Beginn der nächsten Sitzung. Das Zusammenfassen ist eine gute Möglichkeit, Informationslücken und/oder Unstimmigkeiten über das Berichtete festzustellen.

- Zeigen Sie dem Opfer, dass Sie an seiner oder ihrer Geschichte interessiert sind und Anteil nehmen, zum Beispiel, indem Sie nachfragen. Streben Sie nach einem ausgeglichenen Verhältnis zwischen offenen und geschlossenen Fragen. So fördern Sie spontanen Austausch und verhindern, dass sich das Opfer verhört fühlt. Wählen Sie offene Fragen, wenn Sie ein neues Thema beginnen und um das Opfer darin zu bestärken, Informationen preiszugeben. Verwenden Sie geschlossene Fragen, um konkrete und spezifische Informationen zu erhalten.
- Ermutigen Sie das Opfer, seinen oder ihren Emotionen Ausdruck zu verleihen, besonders, wenn sich die Person in einer Krise befindet. Die Fachkraft sollte auf keinen Fall darauf bestehen, dass das Opfer seine oder ihre Emotionen ausdrückt, sofern er oder sie dem nicht zugestimmt hat.

2.3. Informationsbeschaffung als Schlüsselfaktor

Das Sammeln von Informationen ist beim Kontakt zu und der Betreuung von Kriminalitätsopfern, einschließlich Cyberkriminalitätsopfern, ein zentraler Prozess.

Der **erste Kontakt zum Opfer dient der Informationsbeschaffung** über Cyberkriminalität, ihre Auswirkungen und dadurch ausgelöste Bedürfnisse. Jedoch muss berücksichtigt werden, dass das **Sammeln und Analysieren von Informationen wiederkehrende Schritte sind**, die regelmäßiger Bestandteil der Unterstützung und Betreuung von Kriminalitäts- und Cyberkriminalitätsopfern sind.

HIGHLIGHT | WICHTIGSTE INFORMATION:

Es kommt nicht selten vor, dass das Opfer **beim ersten Kontakt mit der Betreuungsfachkraft und/oder der Hilfsorganisation Anzeichen von Unwohlsein und Angst** zeigt.

Fachkräfte sollten berücksichtigen, dass es möglicherweise das erste Mal ist, dass das Opfer über seine oder ihre Cyber-Viktimisierungserfahrung spricht und es völlig normal ist, dass er oder sie Anzeichen von Unwohlsein, Leid und Verletzlichkeit, Zögern und/oder Scham zeigt. Diese Anzeigen können besonders ausgeprägt sein, wenn die Erfahrungen, über die gesprochen werden soll, bestimmte Details aus der Beziehungs- und/oder sexuellen Intimität des Opfers beinhalten.

Die Fachkraft sollte (entsprechend den Informationen aus Tabelle 2):

- Die Sprechpausen, das Zögern und die Erzählgeschwindigkeit des Opfers respektieren.
- Das Opfer ermutigen, sich Hilfe zu suchen und über seine oder ihre Cyber-Viktimisierungserfahrung zu sprechen.
- Dem Opfer erklären und versichern, dass seine oder ihre Reaktionen, Gefühle und Gedanken normal sind, sowohl was das Unwohlsein bezüglich des Offenlegens von Informationen im Beratungskontext betrifft als auch die Cyber-Viktimisierungserfahrung selbst: in jedem Fall handelt es sich um natürliche Reakti-onen auf unerwartete und außergewöhnliche Erlebnisse und Umstände.
- Dem Opfer zeigen, dass er oder sie bereit ist, dem Opfer zuzuhören und ihn oder sie zu unterstützen, einschließlich seiner oder ihrer Ängste, Sorgen und Wünsche.

2. WICHTIGE ASPEKTE FÜR DEN ERSTEN KONTAKT ZU CYBERKRIMINA-LITÄTSOPFERN

Das **Sammeln von Informationen muss dem emotionalen Zustand des Opfers angepasst werden**. Sollte das Opfer nicht in der Lage sein, alle notwendigen Informationen mitzuteilen, sammelt die Fachkraft so viele Informationen wie möglich. Reichen diese nicht aus, sollten weitere Sitzungen vereinbart werden, damit umfassendere Informationen gewonnen werden können.

Das emotionale Wohlbefinden des Opfers hat oberste Priorität, selbst wenn dies auf Kosten der Informationsbeschaffung geht.

Durch die vom Cyberkriminalitätsopfer bereitgestellten Informationen kann die Fachkraft:

1
- Informationen über das Cyber-Verbrechen sammeln, dem das Opfer ausgesetzt war
- Auswirkungen und Folgen für das Cyberkriminalitätsopfer beurteilen

2
- Die Wahrscheinlichkeit einer (erneuten) Viktimisierung, entweder durch Cyberkriminalität oder im herkömmlichen Sinn, einschätzen
- Cybersicherheitsmaßnahmen und schützende, persönliche Routinen im Umgang mit dem Internet etablieren

3
- Die Bedürfnisse des Cyberkriminalitätsopfers identifizieren
- Die entsprechenden Ressourcen und Dienste mobil machen, um die Bedürfnisse des Opfers zu erfüllen und den Auswirkungen der Cyber-Viktimisierungserfahrung zu begegnen bzw. sie zu minimieren

Die Informationsbeschaffung sollte sich auf 3 Bereiche konzentrieren:

1. **Persönliche Vorgeschichte vor der Viktimisierung**
   Die Fachkraft sollte versuchen, Informationen über den familiären, beruflichen und sozialen Hintergrund, Internet- und IKT-Nutzung, Nutzungsgewohnheiten sozialer Netzwerke, riskante Verhaltensweisen/Aktivitäten, ggf. bestehende Cybersicherheitsmaßnahmen und persönliche, schützende Routinen im Umgang mit dem Internet zu erhalten und mögliche vorherige Viktimisierungserfahrungen festzustellen.

2. **Cyber-Viktimisierungserfahrung**
   In diesem Bereich sollten alle verfügbaren Informationen über das Cyber-Verbrechen gesammelt werden, das das Opfer erlebt hat, einschließlich aller Details über die Umstände: was ist passiert; wie ist es passiert; welche IKT- und/oder Internet-basierenden Kommunikationstools wurden verwendet; wem wurden Beweise für das Cyber-Verbrechen zugäng-lich gemacht und über welche Plattform; wer sind die Täter und in welcher Beziehung stehen sie zum Opfer; wann begann die Cyber-Viktimisierung und dauert die Situation noch an; trat die Cyber-Viktimisierung gemeinsam mit anderen Formen der Viktimisierung durch *herkömmliche* Straftaten durch die gleichen oder andere Täter auf; welche Maßnahmen hat das Opfer bereits ergriffen.

3. **Leben nach der Viktimisierungserfahrung**
   Ziel ist die Analyse und Evaluation der Auswirkungen der Cyber-Viktimisierung: das Verstehen der Konsequenzen, Bewältigungsstrategien, Schutzmaßnahmen, die das Opfer ergreifen kann; neben der Beurteilung der Familie, sozialen Unterstützung und der Fähigkeit des Opfers, mit den Folgen zurecht zu kommen und die Kontrolle über sein oder ihr Leben zurückzuerlangen. Die Motivation des Opfers, Präventionsmaßnahmen zu ergreifen und einen Sicherheitsplan auszuarbeiten, muss ebenfalls festgestellt werden.

2.4. Sonderfall: Cyberkriminalitätsopfer im Kindes- und Heranwachsendenalter

Wie in Teil I dieses Handbuchs[81] beschrieben, sind Kinder und Heranwachsende aufgrund ihrer Internet- und IKT-Nutzungsgewohnheiten eine besonders anfällige Gruppe für Cyberkriminalität, auch, weil Erwachsene solche Nutzungsgewohnheiten oft schlecht überwa-chen (besonders im familiären Kontext).

Kontakt zu und Betreuung von Cyberkriminalitätsopfern im Kindes- und Heranwachsendenalter muss:

1. Stets den **Schutz und die Durchsetzung ihrer Rechte** zum Ziel haben;
2. Stets den Persönlichkeitsmerkmalen und zum **Entwicklungsstand** des Kindes oder Heranwachsenden angepasst werden;
3. Sofern möglich, stets die **Einbeziehung der Familie** in Betracht ziehen;
4. Stets den Erwerb von Kompetenzen für eine sichere und bewusste Nutzung des Internets und IKT als Schutzmaßnahme vor einer erneuten Viktimisierung beinhalten.

Auf jeden dieser Punkte soll im Folgenden detailliert eingegangen werden.

1

- **Schutz und Durchsetzung der Rechte eines Kindes während des gesamten Betreuungszeitraums für ein Cyberkriminalitätsopfer im Kindes- oder Heranwachsendenalter**

Beim Kontakt zu und der Betreuung von Kindern und Heranwachsenden, die Kriminalität allgemein oder Cyberkriminalität im Speziellen zum Opfer gefallen sind, müssen Fachkräfte stets die Rechte von Kindern und Heranwachsenden berücksichtigen. Dieses Handbuch wird dieses Thema nicht umfassend erörtern, da die verschiedenen Besonderheiten der nationalen Gesetzgebung jedes Mitgliedsstaats nur schwer berücksichtigt werden können. Stattdessen empfehlen wir dringend,

[81] Siehe Teil I, Abschnitt 3.2 dieses Handbuchs.

dass jede Fachkraft, die Opfer im Kindes- oder Erwachsenenalter kontaktiert oder betreut, die geltenden Gesetze[82] kennt und entspre-chend handelt.

Die UN-Kinderrechtskonvention[83] legt eine Reihe grundlegender, allgemeingültiger Rechte für Kinder fest und enthält einige fundamentale Prinzipien, die auf jegliche Betreuung von Kindern und Heranwachsenden angewendet werden können. Diese lauten

- Die **Wahrung der Interessen der Kinder** beinhaltet die Anweisung, dass alle Gesetze und Handlungen, die Kinder betreffen, die Interessen des Kindes über alle anderen stellen sollen, um ihnen auf die bestmögliche Art zu helfen.
- **Nichtdiskriminierung** bedeutet, dass kein Kind aufgrund von Abstammung, Hautfarbe, Geschlecht, Sprache, Religion, Nationalität, ethnischer oder sozialer Herkunft, politischer oder anderer Werteinstellung, ökonomischem Status oder physischem oder mentalem Zustand benachteiligt (oder bevorzugt) werden darf.
- Das Recht auf **Überleben, Entwicklung und Schutz** verpflichtet alle Behörden dazu, Kinder zu schützen und sicherzustellen, dass sie sich physisch, sozial, spirituell und moralisch entfalten können.
- Das Prinzip der **Beteiligung** räumt Kindern ein Mitspracherecht bei allen Entscheidungen ein, die sie betreffen, und das Recht, in Angelegenheiten, die sie betreffen, angehört zu werden.

Entsprechend sollten die Fachkraft und die Hilfsorganisation die Betreuung in Übereinstimmung mit diesen Grundsätzen und der geltenden Gesetzgebung planen, definieren und umsetzen und stets die Notwendigkeit der Förderung der **vollen Umsetzung der Rechte von Kindern und Heranwachsenden** berücksichtigen.

- **Berücksichtigung des Entwicklungsstands des Kindes oder Heranwachsenden während der Betreuung**

2

Kontakt zu und Betreuung von Cyberkriminalitätsopfern im Kindes- oder Heranwachsendenalter muss zu anderen Bedingungen stattfinden als der zu erwachsenen Opfern.

Fachkräfte müssen die wichtigsten Schritte im **Entwicklungsprozess von Kindern und Heranwachsenden** kennen, besonders im Hinblick auf Sprache und Kommunikation und ihre Kommunikationsstrategien bei der Arbeit entsprechend anpassen (APAV, 2019).

Die folgende Tabelle fast allgemein die wichtigsten Schritte im Entwicklungsprozess von Kindern und Heranwachsenden nach Altersgruppen zusammen.

[82] In Portugal schützen Gesetz Nr. 147/99 vom 1. September über den Schutz von gefährdeten Kindern und Heranwachsenden und seine Zusätze die Rechte von gefährdeten Kindern und Heranwachsenden und stellt ihr Wohlergehen und angemessene Entwicklung sicher. Das Gesetz im Wortlaut ist abrufbar unter https://apav.pt/apav_v3/images/pdf/proteccao_criancas_jovens_perigo.pdf

[83] Im Wortlaut abrufbar unter https://www.ohchr.org/en/professionalinterest/pages/crc.aspx.

Tabelle 4: Wichtigste Entwicklungsphasen von Kindern und Heranwachsenden

	Körperliche Entwicklung	Emotionale und kognitive Entwicklung (einschließlich Sprache)	Soziale und moralische Entwicklung
3 - 6 Jahre	• Malen und andere händische Aktivitäten • Eigenen Namen schreiben • Der Körper entwickelt sich, nimmt erwachsene Züge an • Geschicklichkeit und Koordinationsfähigkeit verbessern sich	• Erinnerung an bekannte Erfahrungen • Verwendung erster Wörter • Sprachliche Anpassung an Merkmale des Gesprächspartners (wie Alter, Geschlecht und sozialer Status)	• Interpretation, Vorausahnen und Beeinflussen der Reaktionen anderer Personen • Aufbau erster Freundschaften • Erste auf sich selbst bezogene Emotionen (wie Scham oder Schuld) • Relative Kontrolle über eigene Gefühle
6 - 12 Jahre	• Starkes Wachstum und Gewichtszunahme • Handschrift wird kleiner und lesbarer • Detailliertere Zeichnungen • Spiele und Witze beinhalten Rennen, Aufregung und Wettbewerb • Motorische Geschicklichkeit ermöglicht schnelle Reaktionsfähigkeit • Erste Anzeichen der Pubertät, besonders bei Mädchen	• Gedanken und Aufmerksamkeit sind fokussierter • Induktives Denken • Verbindung von Erfahrungen mit spezifischen Vorkommnissen • Größerer Wortschatz	• Zunehmende Unabhängigkeit und Verantwortungsbewusstsein • Unterscheidung zwischen Erfolg und Misserfolg • Unterscheidet Handlungsergebnisse anhand von eigener Mühe vs Glück • Hineinversetzen in andere (Empathie)
12 - 18 Jahre	• Pubertät • Menstruation und Zunahme des Körperfettanteils bei Mädchen • Stimmveränderung und Zunahme an Muskelmasse bei Jungen • Zunehmendes Interesse an Sexualität	• Effektive Argumentation • Mehr Bewusstsein für die eigene Persönlichkeit, größere Fokussierung • Entwicklung hypothetisch-deduktiver Argumentationsstrategien • Leichte Veränderungen in der Sprache möglich • Pläne machen und Entscheidungen treffen	• Zunehmende Konflikte mit den Eltern/der Familie • Gesteigerte Nähe zu Gleichaltrigen und Aufkommen von Situationen, in denen durch Gleichaltrige Druck entsteht • Suche nach der eigenen Identität • Aufbau intimer Beziehungen

Die folgende Tabelle gibt eine Übersicht über die wichtigsten Unterschiede beim Kontakt zu und der Kommunikation mit Kindern und Heranwachsenden verschiedener Altersgruppen, die die Fachkraft berücksichtigen muss (APAV, 2011).

Tabelle 5: Kontakt zu und Kommunikation mit Kindern und Heranwachsenden verschiedener Altersgruppen

	1 - 6 Jahre	6 - 12 Jahre	12 - 18 Jahre
Sich vorstellen	Direkt an das Kind gerichtet. Das Kind ist noch zu jung, um die Informationen zu verstehen.	Das Kind zeigt mehr Interesse an den bereitgestellten Informationen und kann sie besser verstehen.	Das Kind/die heranwachsende Person versteht die bereitgestellten Informationen, könnte aber Widerwillen gegen die Teilnahme an einem Interventionsprogramm oder eine Opferberatungsmaßnahme zeigen.
Beschreibung des Ereignisses	Drückt sich lieber durch Malen oder Spielen aus, statt durch Wörter.	Kann detaillierter kommunizieren als jüngere Kinder. Ältere Kinder kommunizieren lieber verbal und weigern sich ggf., zu malen oder Spiele zu spielen.	Detaillierte Beschreibung des Ereignisses. Das Opfer gibt sich selbst die Schuld.
Psychoedukation	An Familie/Eltern gerichtet. Das Kind kann einfache Informationen verarbeiten, wie zum Beispiel die Situation anerkennen, und sich Bewältigungsstrategien vorstellen.	An das Kind gerichtet, unter Einbezug der Familie/Eltern in den Prozess der Psychoedukation.	An/Durch das Kind gerichtet

Unter allen Umständen müssen Fachkräfte beim Kontakt mit oder der Betreuung von Cyberkriminalitätsopfern im Kindes- oder Erwachsenenalter ein angemessenes Umfeld schaffen, indem sie mit den Kindern/Heranwachsenden kommunizieren, um zu verhindern, dass das Opfer eine „polizeiähnliche Verhörsituation" erlebt. Da dies ausdrücklich nicht das Ziel der Maßnahme ist, ist eine angenehme und informelle Umgebung von größter Wichtigkeit. Sie trägt zum Aufbau einer Vertrauensbeziehung zwischen der Fachkraft und den Opfern im Kindes- oder Heranwachsendenalter bei.

Bei jüngeren Kindern kann die Anwesenheit eines Verwandten oder Erziehungsberechtigten erforderlich sein, bis das Kind sich an die Fachkraft gewöhnt hat und sich ohne Beistand durch einen Verwandten oder Erziehungsberechtigten sicher fühlt (APAV, 2019).

- **Einbezug der Familie, wenn möglich**

3

In Fällen von Cyberkriminalität, die sich gegen Kinder und Heranwachsende richtet, spielen **Eltern und Familie eine ausschlaggebende Rolle**. Ihnen kommt eine präventive Rolle zu, indem sie Kinder und Heranwachsende informieren, überwachen und, sofern notwendig, die Nutzung des Internets oder IKT einschränken (Öztürk & Akcan, 2016). Der **Einbezug der Familie in Situationen, in denen**

ein Cyber-Verbrechen bereits stattgefunden hat, ist ebenso wichtig, da:

- Sie über relevante Informationen über die Vorgeschichte des Kindes oder Heranwachsenden verfügen;
- Die Teilnahme des Opfers im Kindes- oder Heranwachsendenalter am Beratungsprozess selbst bzw. deren Häufigkeit zu einem großen Teil von der Verfügbarkeit und Bereitschaft der Eltern oder Familie abhängt;
- Sie Schlüsselelemente für die Psychoedukation der Kinder und Heranwachsenden und für die Verhinderung einer erneuten Viktimisierung sind.

Fachkräfte müssen sich ebenfalls über das Ausmaß bewusstwerden, in dem die Cyber-Viktimisierungserfahrung des Kindes oder Heranwachsenden zu Veränderungen persönlicher, ehelicher oder familiärer Natur in ihrem Umfeld geführt hat. **Die Anerkennung der Auswirkungen der Cyber-Viktimisierungserfahrung auf die Familie wird ebenso zum Heilungsprozess des Kindes beitragen**. Die Reaktionen der Familie auf Cyber-Viktimisierungserfahrungen von Kindern und Heranwachsenden ähneln in jeglicher Hinsicht denen, die in Situationen herkömmlicher Gewalt oder Kriminalität auftreten (APAV, 2011):

- **Wunsch nach Rache**. Der Wunsch nach Rache in Verbindung mit einem Bedürfnis nach Aufbegehren bzw. der Wunsch „die Gerechtigkeit selbst in die Hand zu nehmen" ist eine übliche Reaktion;
- Schuldgefühle. Die Familie fühlt sich u. U. schuldig, weil sie nicht erkannt/geahnt hat, dass das Kind oder der/die Heranwachsende Opfer von Kriminalität oder Gewalt geworden ist;
- „Sensibles Thema". Vielen Familien und Eltern fällt es sehr schwer, mit dem Kind oder dem Heranwachsenden über die Art von Gewalt zu sprechen, der sie zum Opfer gefallen sind. Trotzdem ist diese Art des Dialogs wichtig für die Stärkung der Vertrauensbeziehung zwischen der Familie und dem Kind oder Heranwachsenden. Dies kann jedoch kontraproduktiv sein, wenn die Familie das Kind oder den/die Heranwachsenden zu sehr unter Druck setzt, über die Viktimisierung zu sprechen;
- Veränderung der Beziehung. Die Beziehung zum Kind oder Heranwachsenden kann sich verändern: die Familien-/Eltern-Kind-/Heranwachsendes Opfer- Beziehung kann komplizierter und von Peinlichkeit und gegenseitigen Schuld- und Schamgefühlen überschattet werden;
- Fehlendes Vertrauen in die Betreuung. In vielen Fällen vertraut die Familie den Organisationen nicht, besonders den Polizeibehörden. Ein Grund dafür ist häufig, dass sie keine Informationen über die laufenden Ermittlungen erhalten;
- Umfassende Auswirkungen auf das Leben. Alle Bereiche des persönlichen, sozialen, beruflichen und Familienlebens von Familienmitgliedern und Eltern können betroffen sein.
- Bedarf nach Unterstützung. Zusätzlich zu der Betreuung der Cyberkriminalitätsopfer im Kindes- oder Heranwachsendenalter können deren Familien und Eltern ebenfalls besondere Betreuung benötigen, um sie bei den o. g. Aufgaben und Herausforderungen zu unterstützen.

2. WICHTIGE ASPEKTE FÜR DEN ERSTEN KONTAKT ZU CYBERKRIMINA-LITÄTSOPFERN

Die Handlungen der Fachkraft und der Hilfsorganisation sollten in Fällen von Cyber-Viktimisierung von Kindern und Heranwachsenden neben der Reaktion auf die aus der Konfrontation mit Cyberkriminalität erwachsenden Bedürfnisse auch stets die Förderung sicherer und bewusster Verhaltensweisen im Umgang mit dem Internet und IKT beinhalten – Ziel ist es, die erneute Verwicklung der Kinder oder Heranwachsenden in Risikosituationen oder eine erneute Cyber-Viktimisierung zu verhindern.

Es ist wichtig, dass Opfer im Kindes- und Heranwachsendenalter im sicheren und angemessenen Umgang mit dem Internet und IKT geschult werden. Dies sollte Folgendes beinhalten: Etablierung angemessener Online-Verhaltensweisen für den persönlichen Schutz; die positive und sichere Nutzung des Internets und IKT; Einrichtung von Cybersicherheitsmaßnahmen in IKT und Kommunikations-Tools mit Internetzugang; das Identifizieren von Situ-tionen, die ein hohes Risiko für Cyber-Viktimisierung bergen und entsprechendes Verhalten (Martellozzo & Jane, 2017; Wolak, Finkelhor, Mitchell & Ybarra, 2010; Lwin, Ang & Liu, 2013; Wright, 2015).

HIGHLIGHT | ANGEBOTE IM FOKUS:

Im Vereinigten Königreich stellt das *ThinkUKnow*-Programm auf Kinder verschiedener Altersgruppen sowie Familien, Eltern, Erziehungsberechtigte und Lehrer zugeschnittene Informationen über Cyberkriminalität und Onlinesicherheit zur Verfügung.

Dieses Programm wurde vom *Child Exploitation and Online Protection Centre* (CEOP) ins Leben gerufen und bietet Sicherheitsberatung und Informationen hinsichtlich vieler Themen, die mit der Internet- und IKT-Nutzung zusammenhängen und zu riskanten Situationen führen können (Marczak &Coyne, 2010).

Zugang zur Plattform erhalten Sie unter: www.thinkuknow.co.uk/

3. BETREUUNG VON CYBERKRIMINALITÄTSOPFERN

In diesem Kapitel des Handbuchs widmen wir uns, in Verbindung zu den allgemeinen Richtlinien für Kontakt, Kommunikation und Informationsbeschaffung aus dem vorangegangenen Kapitel, der Betreuung von und Intervention für Cyberkriminalitätsopfer.

Neben den Auswirkungen der Cyber-Viktimisierungserfahrung und dem daraus erwachsenden Bedarf an Unterstützung, die wir in Kapitel 4, Teil I dieses Handbuchs erörtert haben, konzentrieren wir uns auf die emotionale Unterstützung, Krisenintervention und die zentralen Aspekte der professionellen Betreuung von Cyberkriminalitätsopfern.

Angesichts der vielfältigen Arten von Cyberkriminalität möchten wir betonen, dass die hier vorgestellten Inhalte keineswegs die einzig möglichen Handlungsweisen im Umgang mit Cyberkriminalitätsopfern sind. Im Gegenteil, es handelt sich um einen weitreichenden Fahrplan verschiedener Handlungsrichtlinien, die Fachkräften und Organisationen bei der Konzipierung und Umsetzung ihrer Betreuung gemäß ihren eigenen Merkmalen und Zielen helfen können, stets in der Absicht, die Bedürfnisse eines Cyberkriminalitätsopfers bestmöglich zu erfüllen.

HIGHLIGHT | WICHTIGSTE INFORMATION:

Da dieses Kapitel und die vorangehenden im *Betreuungs*-Teil dieses Handbuchs davon ausgehen, dass die Betreuung von Cyberkriminalitätsopfern durch Organisationen, genauer durch Hilfsorganisationen für Opfer, erfolgt, müssen einige **grundlegende Erfordernisse und praktische Aspekte für die Entwicklung und den Betrieb einer Hilfsorganisation für Cyberkriminalitätsopfer** erörtert werden.

Jede Organisation, die ein Hilfs- oder Betreuungsangebot für Cyberkriminalitätsopfer umsetzen will, sollte zunächst eine **diagnostische Beurteilung ihrer organisatorischen Kapazitäten**[84] durchführen.

Einige der Bereiche, die intern geprüft werden sollten, sind:

- Passt das Hilfs- oder Betreuungsangebot zur Mission und den Aktivitäten der Organisation und bestehen gegebenenfalls Synergien mit anderen Angeboten (wie Hilfs- und Betreuungsangebote für Kriminalitäts- und Gewaltopfer);
- Besteht die finanzielle Kapazität für die Entwicklung und den Betrieb eines Hilfs- oder Betreuungsangebots, besonders im Hinblick auf die Existenz eigener Ressourcen, Zugang zu externen Finanzierungsquellen und/oder Sponsoring;
- Besteht Zugang zu materiellen, technologischen und logistischen Ressourcen, die für die Einrichtung und den Betrieb des Hilfs- oder Betreuungsangebots erforderlich sind;
- Besteht ausreichend Kenntnis über die Art von Hilfe, die gewährt werden soll, und über Cyberkriminalität als solches, einschließlich der verschiedenen Formen von Cyberkriminalität, den Risikofaktoren und Auswirkungen von Cyberkriminalität und die geltenden gesetzlichen Rahmenbedingungen;
- Bestehen ausreichend organisatorische und technische Kapazitäten für die Entwicklung von Abläufen, die das Hilfs- oder Betreuungsangebot umfassen soll und entsprechen diese der Mission, den Prinzipien und Werten der Organisation, ihrer anderen Angebote und den geltenden Gesetzen;
- Bestehen (formelle/informelle) Partnerschaften mit anderen Organisationen, die über Erfahrung und Expertise in diesem Bereich verfügen und mit denen eine Zusammenarbeit möglich ist, zum Austausch

[84] Übernommen von Safety Net Project - https://www.techsafety.org/resources-agencyuse

oder Erhalt von Wissen, Erfahrung und bewährter Methoden;
- Ist ausreichend qualifiziertes Personal (angestellt und/oder ehrenamtlich) vorhanden, das diese Art von Betreuung leisten kann, und besteht ausreichend technische und finanzielle Kapazität für deren Vorbereitung und Qualifizierung.

Zusammenfassend muss **die Vorbereitung der Organisation auf die Umsetzung** eines Betreuungs- oder Hilfsangebots für Cyberkriminalitätsopfer die folgenden, grundlegenden Schritte umfassen:

1. Definieren der Ziele des geplanten Hilfs- oder Betreuungsangebots. Diese können zum Beispiel sein: Information/Aufklärung; emotionale Unterstützung; praktische Unterstützung; spezifische Betreuung oder Beratung (z. B. in rechtlichen Angelegenheiten); Empfehlung an andere Angebote/Dienste/Organisationen, die für den Umgang mit der Situation qualifiziert sind.
2. Identifizierung der Empfänger des geplanten Hilfs- oder Betreuungsangebots: Es kann sich um ein Hilfs- oder Betreuungsangebot und/oder Aufklärung für Opfer jegli-cher Art von Cyberkriminalität handeln; oder sich an spezifische Opfergruppen und/oder einzelne Formen von Cyberkriminalität richten. Ein Beispiel hierfür ist die Meldestelle für Inhalte, die sexuellen Missbrauch oder Ausbeutung von Kindern zeigen.
3. Etablierung von Abläufen und Strategien für die Formulierung und Integration der Betreuungs- und Hilfsangebote für Kriminalitätsopfer anderer Organisationen, sofern vorhanden, und Festlegung der Kriterien, wie der interne Umgang mit Informationen über bestimmte Situationen von Cyber-Viktimisierung zu erfolgen hat, um dem Opfer bestmöglich gerecht zu werden. Verbindungen zu und Kooperation mit anderen Institutionen sollte ebenfalls in Betracht gezogen werden[85].
4. Entwicklung spezifischer Abläufe für die angebotene Betreuung unter Berücksichtigung der Ziele und der Empfänger des Hilfs- oder Betreuungsangebots, geltenden Gesetzen[86] und gegebenenfalls beruflicher Verhaltenskodizes. Außerdem sollte die Organisation über gute Kenntnisse über das Phänomen, seine Auswirkungen auf Opfer und die durch Cyber-Viktimisierungserfahrungen ausgelösten Bedürfnisse verfügen[87].
5. Auswahl und Ausbildung personeller Ressourcen für die Umsetzung des Hilfs- oder Betreuungsangebots[88].
6. Bewerben Sie das Hilfs- oder Betreuungsangebot[89].

3.1. Von emotionaler Unterstützung zu Krisenintervention

Kurz gesagt basiert die emotionale Unterstützung eines Cyberkriminalitätsopfers hauptsächlich auf der Umsetzung und Anwendung der in diesem Handbuch bereits erwähnten und im Folgenden aufgeführten Fähigkeiten der Fachkraft:

- **Empathische Kommunikation**, einschließlich aktivem Zuhören;
- **Non-verbale Kommunikation**, die Verfügbarkeit, Offenheit und aktives Zuhören ausdrückt;
- **Anerkennung der Aussage** und **Akzeptanz der Erzählgeschwindigkeit des Opfers**;
- Bestärkung des **Opfers beim emotionalen Ausdrücken und Begreifen** seiner oder ihrer Erfahrung, Reaktionen, Gefühle, Verhaltensweisen, Gedanken und Bedeutung, die er oder sie der Erfahrung zuschreibt.

In diesem Kontext weisen wir erneut darauf hin, dass **emotionale Unterstützung bei der Befragung des Opfers** über dessen Cyber-Viktimisierungserfahrung von elementarer Wichtigkeit ist (nicht zuletzt, weil die

[85] Siehe Abschnitte 3.5.1.3. und 3.5.3.2. In Kapitel 3, Teil II dieses Handbuchs für weitere Informationen über solche Kooperationen.

[86] Siehe Teil I, Kapitel 2 dieses Handbuchs für weitere Informationen zu den rechtlichen Rahmenbedingungen in Bezug auf Cyberkriminalität.

[87] Siehe Kapitel 1, 3 und 4 in Teil I dieses Handbuchs für umfassende Informationen über das Phänomen der Cyberkriminalität, Erklärungsansätze, Risikofaktoren und Auswirkungen.

[88] Siehe Teil II, Kapitel 1 dieses Handbuchs für Informationen über die persönlichen und beruflichen Kenntnisse, die eine Fachkraft für die Betreuung von Cyberkriminalitätsopfern benötigt.

[89] Siehe Teil II, Abschnitt 4.2 dieses Handbuchs für weitere Informationen über die Rolle öffentlicher Informations- und Aufklärungskampagnen für die Verbreitung von Informationen über bestehende Ressourcen zur Unterstützung und zum Schutz von Cyberkriminalitätsopfern. cybercrime.

Informationsbeschaffung durch die daraus folgende Notwendigkeit, von der Cyber-Viktimisierungserfahrung zu erzählen, negative Erinnerungen an und Gefühle hinsichtlich der Cyber-Viktimisierungserfahrung auslösen kann; außerdem ist die Informationsbeschaffung an sich eine unangenehme und entblößende Situation für das Opfer). Entsprechend bleibt die emotionale Unterstützung während des gesamten Betreuungsprozesses des Cyberkriminalitätsopfers wichtig, unabhängig von der Länge der Intervention.

Unter Umständen sucht das Cyberkriminalitätsopfer die Hilfe der Fachkraft oder der Organisation (hauptsächlich Hilfsorganisationen für Opfer) in einer **Krisensituation**.

HIGHLIGHT | WICHTIGSTE INFORMATION:

Durch ihren potenziell ungewöhnlichen und unvorhersehbaren Charakter und die (reale oder wahrgenommene) Bedrohung für die physische und/oder psychische Unversehrt-heit des Opfers kann eine Cyber-Viktimisierungserfahrung zu einer **Krisensituation** führen (APAV, 2013b).

Eine solche Krisensituation zeichnet sich durch die folgenden Merkmale aus:

- **Intensive psychologische Reaktionen**, wie Weinen, Panik, Verwirrung, Verzweiflung, Scham, niedriges Selbstbewusstsein, Schuld, Wut, psychosomatische Störungen[90] und Flashbacks;
- **Sozialer und ökonomischer Druck**, der zu einer emotionalen oder psychischen Blockade führt, und dadurch entsteht, dass das Opfer seine oder ihre **Rechte nicht kennt**.

Dauer und Intensität der Krise hängen vom Grad der Gewalt ab, die dem Opfer angetan wurde, seinen persönlichen Ressourcen für den Umgang mit der Erfahrung und den zur Verfügung stehenden externen Ressourcen, einschließlich (formelle wie informelle) Unterstützung, die nach der Viktimisierung erfahren wurde.

Krisenintervention (oder psychologische Erste Hilfe) ist daher eine intensive, konzentrierte und zeitlich begrenzte Maßnahme, die sich auf die Lösung akuter Probleme und spezifische Ziele konzentriert. Es handelt sich um eine einleitende, praktische und nichtinvasive Unterstützungsmaßnahme in einer Krise oder Notfallsituation.

Die wichtigsten Aufgaben einer Fachkraft, die Kontakt zu einem Cyberkriminalitätsopfer in einer Krisensituation aufnimmt sind daher:

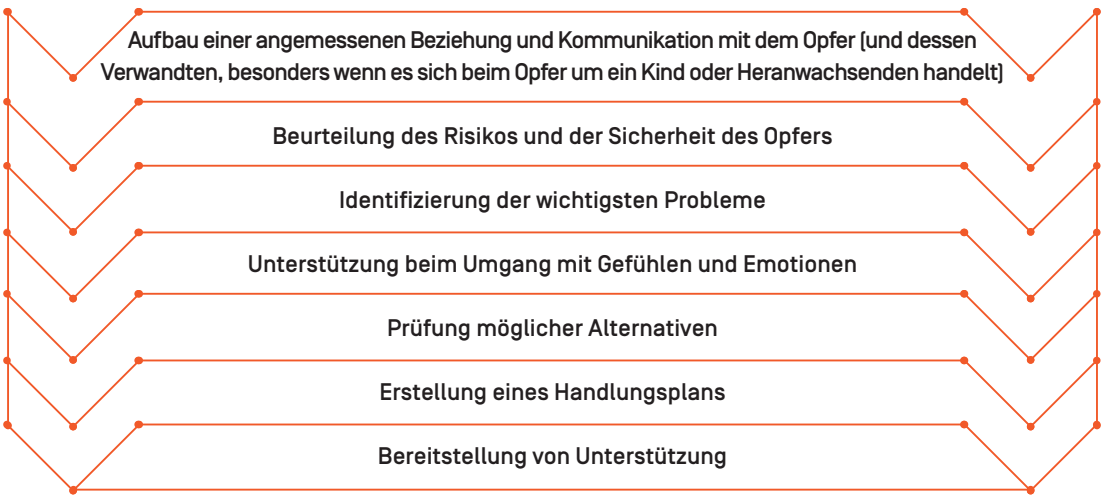
- **Einschätzung der Sicherheit** und **Selbstversorgungskapazität des Opfers** in potenziell traumatischen Situationen unter Berücksichtigung der Tatsache, dass die persönlichen und sozialen Ressourcen, die dem Opfer zur Verfügung stehen, u. U. nicht in der Lage sind, angemessen auf eine höchst fordernde Situation zu reagieren.
- Ergreifung von Maßnahmen, die die **Erholung und Reorganisation des Opfers** zum Ziel haben, den negativen Einfluss der Cyber-Viktimisierung begrenzen und Sicherheit und physisches wie psychologisches Wohlergehen des Opfers sicherstellen.

[90] Psychosomatische Störungen beschreiben die physischen Folgen (z. B. Übelkeit und Magenschmerzen) psycho-logischer Probleme und Störungen.

In Übereinstimmung mit den allgemeinen Richtlinien für die Betreuung von Cyberkriminalitätsopfern (siehe Tabelle 2) sollte Krisenintervention die folgenden Ziele haben:

- Das Opfer ist kein „Einzelfall";
- Behandlung der Suche nach Erklärungen;
- Behandlung der Schuldgefühle des Opfers;
- Das Opfer darf nicht zum Schweigen gebracht oder unter Druck gesetzt werden, „zu vergessen";
- Hoffnung auf Heilung und Lösung des Problems stiften;
- Erklärung der notwendigen rechtlichen Verfahren.

Entsprechend muss die Krisenintervention auf den folgenden **Schritten** basieren:



Bei dieser Art von Intervention empfehlen wir die Umsetzung der o. g. Strategien, ohne Bezug auf weitere, die u. U. hilfreich sein können (APAV, 2013b):

Aufbau einer Beziehung zum Opfer:
Die Fachkraft muss versuchen, eine Vertrauensbeziehung zum Opfer aufzubauen und herausfinden, welche Ereignisse letztlich dazu führten, dass das Opfer Hilfe suchte, um so die Hauptprobleme feststellen zu können.

Beurteilen:
Fachkräfte müssen den mentalen Gesundheitszustand des Opfers kennen, ob er oder sie Suizidgedanken hegt, in welchem Ausmaß Unwohlsein, Beunruhigung und Angst empfunden werden und besonders, ob der geistige Zustand des Opfers ihm oder ihr erlaubt, angemessen mit den

praktischen Verpflichtungen zurechtzukommen, die aus der Cyber-Viktimisierung entstehen.

Die Fachkraft muss außerdem das Risiko (weitere Informationen finden Sie in den folgenden Kapiteln dieses Handbuchs) und das Vorhandensein bzw. die Qualität der Unterstützung durch das primäre Unterstützungsnetzwerk (Familie und/oder Freunde) beurteilen.

Stress und Verzweiflung reduzieren:
Es ist normal, dass das Opfer Stress und Verzweiflung empfindet. Diese Symptome können durch eine Sicherheit vermittelnde, bestärkende Kommunikation reduziert werden. Bei der Kontaktaufnahme sollte die Fachkraft das Opfer darauf hinweisen, dass seine oder ihre Reaktionen normal und gerechtfertigt sind und üblicherweise bei negativen, herausfordernden und/oder anstrengenden, persönlichen Erfahrungen auftreten.

Die Fachkraft soll in dieser Situation auf möglichst natürliche Weise mit dem Opfer kommunizieren (ohne die Ernsthaftigkeit der erlebten Situation zu verleugnen), ihm oder ihr Aufmerksamkeit schenken und keinesfalls ängstliches oder emotional gestörtes Verhalten bestärken.

Interesse zeigen und das Opfer motivieren:
Die Fachkraft muss Interesse, Zuhörbereitschaft und Verständnis für das Opfer und dessen Situation zeigen (siehe Abschnitt 2.2 über Empathie in diesem Teil des Handbuchs). Die Fachkraft sollte ebenfalls Hoffnung auf eine positive (aber realistische) Lösung der Situation schüren, die das Selbstbewusstsein des Opfers stärkt.

Es ist auch wichtig, das Opfer dazu zu ermutigen, eigene Bewältigungsstrategien für seine oder ihre Cyber-Viktimisierungserfahrung zu finden, indem man deren körperliche und geistige Kapazitäten stärkt.

Klären:
Es muss geklärt werden, welche Anforderungen das Opfer als Folge Cyber-Viktimisierung erfüllen muss, einschließlich praktischer Verpflichtungen wie beispielsweise die Kontaktaufnahme zu Banken bei finanziell motivierten Cyber-Verbrechen oder zu Plattformen, um die Löschung illegaler Inhalte einzufordern.

Opfer über Rechte informieren und darin bestärken:
Die Fachkraft muss das Opfer über seine oder ihre Rechte informieren, über die Funktionsweise des Rechtssystems und die Vor- und Nachteile einer Anzeige der Straftat, also insgesamt dazu beitragen, dass das Opfer in dieser Situation eine fundierte Entscheidung treffen kann. Einer der Vorteile der Erstattung einer Anzeige kann sein, dass das Opfer sicher sein kann, aktiv etwas gegen den oder die Täter unternommen zu haben. Ein weiterer Vorteil, den die Fachkraft betonen kann, ist, dass eine Meldung des Verbrechens bei den Behörden dazu beiträgt, Cyberkriminalität zu verhindern und anderen eine ähnliche Cyber-Viktimisierungserfahrung zu ersparen. Schwierigkeiten während des Strafverfolgungsprozesses im Hinblick auf Probleme bei der strafrechtlichen Untersuchung oder der emotionalen Belastung des Opfers selbst, zum Beispiel durch Schamgefühle oder die Notwendigkeit, die traumatische Erfahrung jedes Mal erneut zu durchleben, wenn er oder sie darüber berichten muss, können Nachteile sein.

Die Fachkraft muss das Opfer darauf hinweisen, dass er oder sie die Beweise für die Straftat aufbewahren muss, sofern er oder sie Zugang dazu hat (wie zum Beispiel Links, über die auf Informationen über die Online-Aggression zugegriffen werden kann, der er oder sie zum Opfer gefallen ist, aber auch Nachrichten, Videos und/oder andere Dateien, die er oder sie während der Cyber-Viktimisierung erhalten haben, oder Ausdrucke/Kopien, die die Verbreitung der aggressiven Inhalte im Internet beweisen).

Weiterleitung an Justiz- und Polizeibehörden:
Sollte das Opfer zu dem Zeitpunkt, an dem er oder sie professionelle Hilfe sucht, die Untersuchung der Verbrechen durch Justiz- und Polizeibehörden noch nicht in die Wege geleitet haben, kann die Fachkraft mit dem Einverständnis des Opfers diesen Vorgang erleichtern. Für diesen Fall ist es von größter Wichtigkeit, dass die Hilfsorganisation, für die die Fachkraft tätig ist, Abläufe für die Vereinfachung der Zusammenarbeit mit Organisatio-nen und Behörden definiert und umsetzt, was ebenso in diesem Handbuch thematisiert wird (siehe Abschnitte 3.5.1.3. Und 3.5.3.2. in diesem Kapitel, Teil II dieses Handbuchs).

Unterstützung anbieten:
Die Fachkraft sollte dem Opfer sämtliche Dienste und Hilfsangebote zugänglich machen, zu denen die Organisation Zugang hat. Dies kann auch die Weiterempfehlung an spezifischere Hilfsangebote der eigenen Organisation oder externe, verfügbare Ressourcen auf lokaler, regionaler oder nationaler Ebene sein, im Rahmen organisationsübergreifender Zusammenarbeit.

HIGHLIGHT | ANGEBOTE IM FOKUS:

In Portugal koordiniert APAV ein Netzwerk aus Spezialisten zur Unterstützung von Opfern sexueller Gewalt im Kindes- und Heranwachsendenalter, das sog. CARE Netzwerk, das Opfern sexueller Gewalt im Kindes- und Heranwachsendenalter, aber auch Verwandten und Freunden psychologische, soziale und rechtliche Betreuung bietet.

Dieses Netzwerk verfügt über spezialisierte Fachkräfte im gesamten Staatsgebiet, um eine möglichst hochwertige, dezentralisierte Betreuung anbieten zu können. Das CARE Netzwerk bietet außerdem ortsungebundene Beratungsstellen, an denen Fachkräfte die Bereitstellung multidisziplinärer Unterstützung für Opfer im Kindes- und Heranwachsendenalter, ihre Familien und Freunde gewährleisten, die an deren individuelle Bedürfnisse angepasst und in der Nähe des jeweiligen Wohnorts liegen.

Erhält die Dienststelle eines anderen APAV-Programms Kenntnis von einem Fall von sexueller Gewalt gegen Kinder oder Heranwachsende - zum Beispiel ein Hilfszentrum für Opfer oder die Notfall-Hotline für Opfer | 116 006 - wird dieser Fall (intern) an die Fachkräfte des CARE Netzwerks weitergeleitet.

Weitere Informationen über die Tätigkeit des CARE Netzwerks von APAV finden Sie unter www.apav.pt/care.

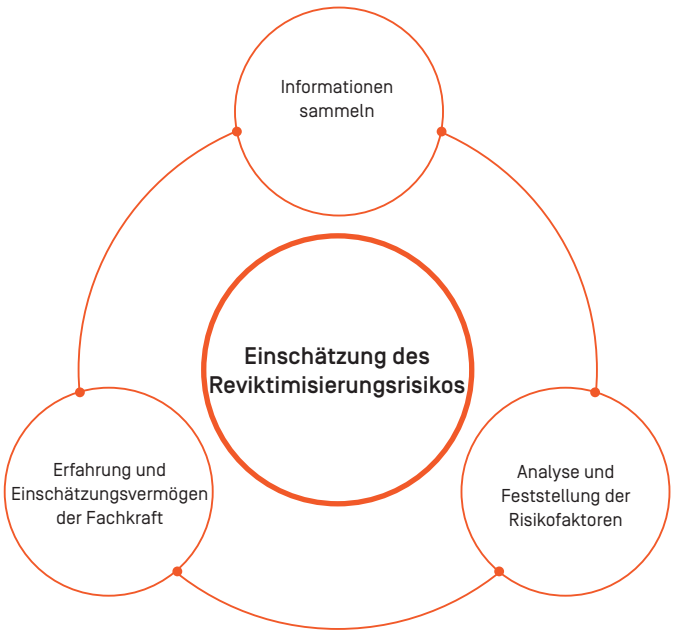
Nach der Krisenintervention kann es notwendig sein, die Betreuung des Cyberkriminalitätsopfers aufrechtzuerhalten, um seine oder ihre Heilung zu fördern und Bedürfnisse zu erfüllen. In Übereinstimmung mit den Betreuungsangeboten anderer Opferhilfsorganisationen für andere Formen der Viktimisierung

behandelt dieses Handbuch auch die zentralen Aspekte spezialisierter rechtlicher, psychologischer und sozialer Intervention, abgestimmt auf die gewöhnlich vorkommenden Bedürfnisse von Kriminalitätsopfern. Die zentralen Aspekte spezialisierter Intervention werden in Abschnitt 3.5 dieses Kapitels erörtert.

3.2. Einschätzung des Reviktimisierungsrisikos

Die Einschätzung des Reviktimisierungsrisikos beurteilt die **Wahrscheinlichkeit einer erneuten Cyber-Viktimisierung des Opfers**. Nach der Informationsbeschaffung (siehe Kapitel 2 dieses Teils des Handbuchs) muss die Fachkraft basierend auf den während der Intervention erhaltenen Informationen die Risiko- und Schutzfaktoren des Opfers[91] beurteilen, damit die Notwendigkeit von Unterstützungs- und Interventionsmaßnahmen festgestellt werden kann.

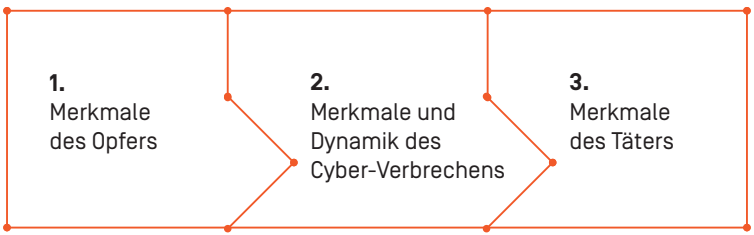
Die Beurteilung des Reviktimisierungsrisikos beruht auf den **Informationen, die das Opfer hinsichtlich seiner oder ihrer Cyber-Viktimisierungserfahrung angegeben hat**, und der Verwendung dieser Informationen für die **(mehr oder weniger strukturierte) Identifizierung der Risikofaktoren für eine Reviktimisierung** (die bei der Planung der Intervention, persönlicher Schutzmaßnahmen im Internet und Cybersicherheitsmaßnahmen besonders berücksichtigt werden, um eine Reviktimisierung zu verhindern). Die **Erfahrung und das Einschätzungsvermögen der betreuenden Fachkraft** sind wichtige Bestandteile des Risikobeurteilungsprozesses.



[91] Detaillierte Informationen über Risikofaktoren für Cybermobbing finden Sie in Teil I, Kapitel 3 dieses Handbuchs.

Wie in Kapitel 3, Teil I dieses Handbuchs beschrieben, ist die Erforschung der Risikofaktoren in Zusammenhang mit Cyber-Viktimisierung bisher nicht weit fortgeschritten und obwohl weitere Faktoren oder Variablen entdeckt werden können, konnten **das Verhalten des Opfers betreffende, individuelle Faktoren** ermittelt werden, die ein erhöhtes Risiko für Cyberkriminalität bzw. Cyber-Viktimisierung zur Folge haben, wie beispielsweise die Nutzungsintensität und -gewohnheiten bezüglich Internet und IKT sowie die Art der Online-Aktivitäten (Wilsem, 2013; Brown et al., 2017; van der Wagen & Pieters, 2018). Die Vielzahl der verschiedenen Arten von Cyberkriminalität macht es schwierig, eine Gruppe von Risikofaktoren oder Variablen festzulegen, die gleichermaßen für alle Arten von Cyberkriminalität zutreffen.

Trotzdem können wir sagen, dass sich die Beurteilung des Reviktimisierungsrisikos auf **drei Risikobereiche** konzentrieren sollte:



Hinsichtlich der vielfältigen Natur der Cyberkriminalität ist klar, dass sich zum Beispiel die Erhebung von Informationen, die eine Betrachtung des Falls aus drei Perspektiven (ausgehend von den Charakteristika des Opfers, Täters und der Dynamik des Cyber-Verbrechens) für die **Analyse des Reviktimisierungsrisikos von Computern und Computersystemen für Cyberkriminalität** (Straftaten, deren Ausübung direkt von Cybertechnologie abhängt)[92] schwierig gestaltet. In solchen Fällen handeln Täter anonym, weshalb ihre tatsächliche Identität schwer festzustellen ist, was wiederum die Analyse ihrer Merkmale und ihres Beitrags zur Erhöhung/Reduzierung des Reviktimisierungsrisikos negativ beeinflusst.

Andererseits ist die Identifizierung und Analyse des Risikos auf drei Ebenen bei der Feststellung der Anfälligkeit des Opfers für eine **Reviktimisierung durch Cyber-Verbrechen, die mittels Computer und Informationssystemen verübt werden**,[93] nützlicher, besonders in Fällen, in denen es eine Beziehung (online und/oder offline) zwischen dem Opfer und dem Täter gibt, da es sich bei diesen häufig um eine Verlagerung *herkömmlicher* Kriminalität in den Cyberspace handelt.

In der folgenden Tabelle sind einige Variablen und Risikofaktoren zusammengestellt, die mit jedem der o. g. Risikobereiche in Verbindung gebracht werden und daher von Fachkräften für die Beurteilung des Reviktimisierungsrisikos des Opfers herangezogen werden können. Es handelt sich hierbei um indikative, allgemeine Variablen, die die spezifischen Dynamiken einzelner Fälle von Cyber-Viktimisierung nicht berücksichtigen.

[92] Siehe Teil I, Kapitel 1 dieses Handbuchs für detaillierte Informationen über diese Konzeptualisierung.

[93] Ditto.

Tabelle 6: Vorgeschlagene Variablen zur Beurteilung des Reviktimisierungsrisikos des Cyberkriminalitätsopfers

Merkmale des Opfers	Merkmale des Cyber-Verbrechens
Risikofaktoren, die von den sozio-demografischen und individuellen Merkmalen des Opfers abhängen und solche, die von den Internet- und IKT-Nutzungsgewohnheiten abhängen.	*Charakteristika und Dynamik des Cyberverbrechens, einschließlich der (online und/oder offline) Beziehung/ Verbindung zwischen Täter und Opfer, besonders im Hinblick auf Cyberkriminalität, die durch das Internet und IKT vereinfacht wird.*
Alter *Bei Kindern/Heranwachsenden und älteren Menschen wurden verschiedene Risikostufen für Cyber-Viktimisierung festgestellt; bei ersteren durch die intensive Internet- und IKT-Nutzung, bei Letzteren durch mangelnde Technikkompetenz.*	**Opfer kennt den cyberkriminellen Täter** *Das Reviktimisierungsrisiko ist höher, wenn sich Täter und Opfer kennen (online und/oder offline). In diesen Fällen verfügt der Täter über mehr Informationen über den Alltag des Opfers (sowohl online als auch offline), was das Reviktimisierungsrisiko erhöht.*
Geschlecht *Die Forschung und Prävalenz-Studien bieten keine übereinstimmenden Erkenntnisse und dieser Faktor sollte vorsichtig interpretiert werden. Obwohl man dem weiblichen Geschlecht eine höhere Viktimisierungsrate bei verschiedenen Cyber-Verbrechen nachsagt, könnte dies an einer höheren Meldequote liegen. Bei einigen Cyber-Verbrechen treten zudem bei männlichen Opfern stärkere Formen von Aggression gegen die Opfer auf.*	**Beziehung zum cyberkriminellen Täter** *Hatten Opfer und Täter eine wie auch immer geartete Beziehung in der realen Welt (frühere Lebenspartner, Kollegen, Freunde), ist das Reviktimisierungsrisiko größer.*
Weitere individuelle Faktoren, die zu einem höheren Viktimisierungsrisiko führen	**Der cyberkriminelle Täter hat eine einschlägige Vorgeschichte** *Hat der Täter bereits früher ähnliche Taten begangen, deutet dies auf ein bestehendes Reviktimisierungsrisiko hin. Einer der zuverlässigsten Indikatoren für das künftige Verhalten des Täters ist sein Verhalten in der Vergangenheit.*
Mentale und/oder kognitive Probleme/Behinderung *Diese Charakteristika können die Fähigkeit des Opfers, Cyber-Viktimisierung zu erkennen, oder sich nach einer Cyber-Viktimisierungserfahrung Hilfe zu suchen, einschränken oder verhindern und so zu einem erhöhten Risiko für eine erneute Viktimisierung führen.*	**Schwere und Auswirkungen des Cyber-Verbrechens** *Die Tatsache, dass das Cyber-Verbrechen Symptome emotionaler und psychologischer Störungen (wie Panikattacken, Angstzustände, Flashbacks, Albträume, Traurigkeit oder weitere Symptome/Anzeigen) ausgelöst hat, kann die Fähigkeit des Opfers beeinträchtigen, sich in der momentanen oder künftigen Viktimisierungssituationen Hilfe zu suchen.*
Hauptsprache *Unterscheidet sich die Hauptsprache des Opfers von der Sprache, in der die Hilfeleistung oder Anzeige von Cyberkriminalität erfolgt, ist das Risiko einer erneuten Viktimisierung größer und es besteht eine größere Anfälligkeit für sozialen Ausschluss und Isolation.*	**Dauer und Eskalationsgrad des Cyber-Verbrechens** *Dauert die Cyber-Viktimisierung an – wie es bei Cyberstalking häufig der Fall ist – und steigt das Maß an Aggressivität und Übergriffigkeit der illegalen Taten gleichzeitig an, so verstärkt dies das Verhalten des Täters und damit das Risiko für das Opfer.*
Vorangegangene Viktimisierungserfahrungen *Ist das Opfer in der Vergangenheit bereits Ziel von Cyberkriminalität gewesen, könnte das Reviktimisierungsrisiko grö-ßer sein, besonders wenn sich die Risikofaktoren nicht verändert haben.*	**Angst vor dem cyberkriminellen Täter** *Die wahrgenommene Angst des Opfers vor dem Täter, besonders wenn diese sich kennen, ist ein wichtiger Indikator, obwohl es auch Situationen gibt, in denen das Opfer das Risiko unterschätzt.*
Keine informelle Unterstützung (z. B. Familie, Freunde, Kollegen) *Soziale Isolation, besonders die Abwesenheit enger sozialer Bindungen, ist ein Risikofaktor für Viktimisierung*	**Vorangegangene (gescheiterte) Lösungsversuche** *Zusätzlich zur Entmutigung des Opfers ermutigt ein solcher Fehlschlag den Täter, weitere Taten gegen das Opfer zu begehen, was das Risiko erhöht.*
Risikofaktoren in Zusammenhang mit dem Internet- und IKT-Nutzungsverhalten	**Meldung/Anzeige** *Die Meldung einer Tat bedeutet für das Opfer stets ein Risiko, da sich der Täter dafür rächen könnte.*
Technikkompetenz *Kompetenz im Umgang mit dem Internet und IKT scheint das*	

Risiko der Cyber-Viktimisierung zu senken. Ist diese nicht oder nur eingeschränkt vorhanden, steigt das Risiko.

Häufigkeit der Internet- und IKT-Nutzung
Personen, die das Internet und IKT häufiger nutzen (z. B. täglich), weisen ein höheres Risiko für Cyber-Viktimisierung auf.

Übliche Online-Aktivitäten/regelmäßig konsumierte Inhalte
Ein hoher Grad an Enthemmung im Online-Verhalten und bei Online-Interaktionen sowie riskante Verhaltensweisen (wie das Herunterladen von Dateien unbekannter Herkunft) werden mit einem erhöhten Risiko für Cyber-Viktimisierung in Verbindung gebracht

Merkmale des Täters

Persönliche und soziale Merkmale eines cyberkriminellen Täters, seine oder ihre kriminelle Vorgeschichte und andere Anzeichen für Gefahr, die auf ein höheres Reviktimisierungsrisiko für das Opfer hindeuten, besonders wenn das Cyber-Verbrechen durch das Internet und IKT ermöglicht oder vereinfacht wurde.

HINWEIS: Zusätzlich zu den o. g. Schwierigkeiten im Hinblick auf die verschiedenen Typologien der Cyberkriminalität reichen die vom Opfer angegebenen Informationen ggf. nicht aus, um die im folgenden aufgeführten Faktoren zu beurteilen.

Etwaige **psychische Probleme und/oder Drogenmissbrauch** seitens des Täters (dem Opfer bekannt)

Etwaige **kriminelle oder anderweitige Vorgeschichte mit den Behörden** seitens des Täters (dem Opfer bekannt)

Versuche, das Opfer zu **kontaktieren oder einzuschüchtern**, nachdem dieses sich Hilfe gesucht hat

Der Wunsch des Täters nach Rache, besonders wenn Täter und Opfer vorher eine intime Beziehung hatten und die Cyberkriminalität eine Form der Vergeltung für das Ende der Beziehung ist (zum Beispiel das nichteinvernehmliche Veröffentlichen von Bildern und Videos)

Besonderes Interesse an Cyberkriminalität, z. B. aus finanziellen Motiven oder Sensationsgier

HIGHLIGHT | WICHTIGSTE INFORMATION:

Die Fachkraft (und die Organisation, für die er oder sie arbeitet) muss festlegen, wie die Informationsbeschaffung für die Beurteilung des Reviktimisierungsrisikos erfolgen soll. Allgemein gilt:

- Die Informationsbeschaffung kann indirekt durch die Fachkraft erfolgen, indem er oder sie die beim Erstkontakt zur Organisation oder Fachkraft des Opfers zur Verfügung gestellten Informationen nutzt;
- Die Beurteilung des Reviktimisierungsrisikos kann auch strukturierter erfolgen, durch konkrete Fragen in Bezug auf die o. g. Variablen (oder anderen, die als relevant angesehen werden) und/oder spezifische Instrumente.

Es muss berücksichtigt werden, dass **die Beurteilung des Reviktimisierungsrisikos nur sinnvoll ist, wenn sie von Maßnahmen begleitet wird, die das Opfer im Umgang mit der Situation und dem Risiko unterstützen**, um seine oder ihre Sicherheit zu gewährleisten und eine erneute Viktimisierung zu verhindern.

Bei der Festlegung der Parameter und Variablen zur Beurteilung des Risikos sollte die Organisation und/oder die Fachkraft ebenfalls die Entwicklung eines Informations- und Sicherheitsplans für das Opfer unter Berücksichtigung der identifizierten Risikofaktoren in Erwägung ziehen. Der **Sicherheitsplan** beinhaltet eine

Reihe von Strategien für die Reviktimisierungsprävention, auf die sich Opfer und Fachkraft gemeinsam geeinigt haben, wie Schutzmaßnahmen und schützende Verhaltensweisen gegen neue Verbrechenssituationen und praktische Anweisungen für den Umgang mit ggf. erneutem Auftreten von Cyber-Viktimisierung.

Abhängig von der Art des Cyber-Verbrechens kann der Sicherheitsplan (Finn & Banach, 2000) folgendes beinhalten:

- Die Umsetzung von Sicherheitsmaßnahmen und schützenden Verhaltensweisen zur Verhinderung einer Reviktimisierung, wie zum Beispiel: Speicherung wichtiger Informationen in passwortgeschützten Dateien und Verzeichnissen; Verschlüsselung der wichtigsten Daten; Vermeidung von Login und/oder Freigabe von persönlichen Informationen in der Öffentlichkeit; Vermeidung offener W-LAN-Netzwerke; Passwortänderungen; Updates für Antivirenprogramme; Änderung der Privatsphäre-Einstellungen in sozialen Netzwerken;
- Identifizierung der Anzeichen für ein Cyber-Viktimisierungsrisiko, wie zum Beispiel: ständige Weiterleitung auf dubiose/unbekannte Webseiten; Pop-Up-Fenster; Herunterladen bzw. Installation dubioser Bilder, Audiodateien oder Anwendungen ohne Einwilligung etc.;
- Praktische Informationen darüber, wie und wo man in einer Viktimisierungssituation Hilfe erhält.

3.3. Beurteilung und Feststellung des Unterstützungsbedarfs

Nach der Zusammenstellung der Informationen mit dem Opfer und der Beurteilung der Ergebnisse der Reviktimisierungsrisikoermittlung muss die Fachkraft den Unterstützungsbedarf des Cyberkriminalitätsopfers ermitteln.

Einige der Aspekte, die der Fachkraft bei der Bedarfsermittlung helfen können, sind die folgenden:

- In welchem Ausmaß und auf welche Weise fühlt sich das Opfer durch die Auswirkungen der Straftat/des Cyber-Verbrechens beeinträchtigt?
- Wie wirkt sich die Cyber-Viktimisierungserfahrung auf das psychische und emotionale Wohlbefinden bzw. Zurechtkommen des Opfers aus?
- Wie wirkt sich die Cyber-Viktimisierungserfahrung auf die körperliche Gesundheit des Opfers aus?
- Wie wirkt sich die Cyber-Viktimisierungserfahrung auf das Verhalten des Opfers in Beziehungen und im beruflichen, sozialen und Arbeitskontext aus?
- Inwiefern beeinflusst die Cyber-Viktimisierungserfahrung den Alltag und die Lebensqualität des Opfers (allgemeines Wohlbefinden)?
- Inwiefern beeinflusst die Cyber-Viktimisierungserfahrung die persönliche Wahrnehmung von Sicherheit und Cybersicherheit (einschließlich der Angst vor Verbrechen)?

- In welchem Ausmaß und auf welche Art und Weise betrifft die Cyber-Viktimisierungserfahrung dem Opfer nahestehende Personen?
- Welche Bedürfnisse hat das Opfer nach der Cyber-Viktimisierungserfahrung?

Abhängig von den Antworten auf die o. g. Fragen sollte die Fachkraft zusammen mit dem Opfer klären, ob:

- es nötig ist, Sicherheitsstrategien für mögliche weitere Straftaten mit dem Opfer zu erarbeiten.
- es nötig ist, dem Opfer die Kontaktaufnahme mit der Polizei/den Justizbehörden zu empfehlen.
- es nötig ist, dem Opfer weitere Unterstützung, Aufklärung und/oder Betreuung nahezulegen (z. B. rechtlich, medizinisch, psychologisch, oder andere).
- es nötig ist, dem Opfer die Weiterleitung seines oder ihres Falls an andere Hilfsdiens-te oder -organisationen nahezulegen (z. B. für spezifische medizinische/psychiatrische Hilfe).

HIGHLIGHT | ANGEBOTE IM FOKUS:

Im Rahmen des EVVI-Projekts (*EValuation of VIctims*) des französischen Justizministeriums wurden ein individueller Fragebogen zur Feststellung der Bedürfnisse eines Opfers und ein praktischer Leitfaden entwickelt.

Dieses Werkzeug für die Ermittlung der Bedürfnisse des Opfers ist in verschiedene Bereiche gegliedert:

- Individuelle Merkmale des Opfers und persönliche Verletzlichkeit wie u. a. Alter, Geschlecht, Ethnie, körperliche oder kognitive Einschränkungen oder Behinderungen;
- Viktimisierungsrisiko und Angst vor Kriminalität, einschließlich der Art und Ursache der Straftat und ihre Umstände;
- Beurteilung der derzeitigen Situation des Opfers;
- Vorgeschichte hinsichtlich Viktimisierung und Informationen über den Täter.

Der Leitfaden und der Fragebogen sind abrufbar unter: http://www.justice.gouv.fr/publication/evvi_guide_en.pdf

Einige der festgestellten Bedürfnisse können über die Dienste und Hilfsprogramme der Organisation abgedeckt werden, die das Cyberkriminalitätsoper betreut.

Andere Bedürfnisse (z. B. medizinische oder psychotherapeutische Betreuung) können **organisationsübergreifende Zusammenarbeit und Kooperationen mit anderen Strukturen**, wie dem Justizsystem oder anderen Systemen, erfordern. Bereichsübergreifende Partnerschaften, einschließlich der zwischen staatlichen, zivilen und Freiwilligenorganisationen, scheinen die Flexibilität und Zugänglichkeit zu Diensten und Betreuungsangeboten zu verbessern und daher dazu beizutragen, die Bedürfnisse der Cyberkriminalitätsopfer besser zu erfüllen (Wedlock & Tapley, 2016).

HIGHLIGHT | WICHTIGSTE INFORMATION:

Die Kapazität einer Organisation, die Bedürfnisse eines Cyberkriminalitätsopfers zu erfüllen, hängt von mehreren Faktoren ab:

- Kompetenz und Mission der Organisation;
- Vorhandensein/Verfügbarkeit von Hilfs- oder Betreuungsangeboten der Organisation, an die die Fachkraft das Cyberkriminalitätsopfer für spezifische Betreuung verweisen kann;
- Beratungsangebote für den Umgang mit Behörden (z. B. Gesundheitsbehörden, Sozialhilfe, Justiz und Sicherheit) und evtl. sogar Protokolle für die institutionsübergreifende Zusammenarbeit[94].

3.4. Die Rolle von Online-Hilfsangeboten bei der Unterstützung von Cyberkriminalitätsopfern

Bis hierher wurden in diesem Handbuch Kontakt zu und Unterstützung von Cyberkriminalitätsopfern unter der Annahme erörtert, dass Unterstützung, Aufklärung und Intervention auf herkömmliche Weise stattfinden (d. h. persönlich oder am Telefon). Aber nicht nur Kriminalität und Gewalt überschreiten physische und konventionelle Grenzen und ermöglichten dadurch die Entstehung von Cyberkriminalität und verschiedener ähnlicher Phänomene, auch die Kontakt- und Unterstützungsmöglichkeiten für Kriminalitätsopfer entwickeln sich weiter.

Opferhilfsorganisationen stellen immer häufiger Informationen und Unterstützung über Online-Hilfsangebote zur Verfügung.

Entsprechend kann auch die Unterstützung für Cyberkriminalitätsopfer entweder auf herkömmliche Weise (einschließlich persönlichem und telefonischem Kontakt) erfolgen, oder über Online-Hilfsangebote, die als gleichwertiger Zugang zu vielen verschiedenen Diensten gelten (Dooley et al., 2010).

Daher sollte mit einigen Vorurteilen gegen Online-Hilfsangebote aufgeräumt werden.

Online-Hilfsangebote ist eine allgemeine Bezeichnung für alle Formen der Unterstützung, Information und/oder Intervention, die online über das Internet und IKT erfolgen (Mallen, Vogel, Rochlen, & Day, 2005, Barak, Klein, & Proudfoot, 2009 cit in APAV, 2017).

Diese Bezeichnung umfasst eine vielfältige Auswahl an Methoden, einschließlich Interventions- oder Unterstützungsmechanismen, die mit oder ohne Interaktion zwischen dem Nutzer und einer Fachkraft funktionieren. Die verschiedenen Unterstützungsmethoden über das Internet unterscheiden sich nicht nur hinsichtlich der (Nicht-) Existenz der Interaktion mit einer Fachkraft, sondern auch im Hinblick auf das Kommunikationsmittel (z. B. Audio, Video und/oder Text), die Art,

[94] Siehe Abschnitte 3.5.1.3. und 3.5.3.2. dieses Kapitels von Teil II des Handbuchs für Informationen über interinstitutionelle Kooperation und Netzwerke.

wie sie andere Formen der Unterstützung/Intervention ergänzen und die Art, wie die Kommunikation stattfindet (gleichzeitig oder zeitversetzt) (Robinson, 2009, Callahan & Inckle, 2012 cit *in idem*).

Es gibt verschiedene Formen von Online-Hilfsangeboten: Internetbasierte Interventions-/Unterstützungsprogramme; Online-Betreuung; Blogs, Online-Foren und Selbsthilfegruppen; Online-Software; andere Formen sich selbst verwaltender Online-Hilfsangebote (Ba-rak et al., 2009, Dowling, & Rickwood, 2013 *cit in idem*).

Unter den verschiedenen Formen der Online-Hilfsangebote kommt die **Online-Unterstützung** einer Online-Version der herkömmlichen Hilfs- und Informationsangebote und/oder persönlicher Intervention am nächsten.

Online-Unterstützung bezieht sich auf die Bereitstellung von Unterstützung und/oder Informationen für Cyberkriminalitätsopfer auf die folgende Art (APAV, 2019):

- Die Kommunikation erfolgt über Internet und IKT;
- Unterstützung und/oder Informationen werden remote zur Verfügung gestellt (d. h. über eine Distanz), Fachkraft und Opfer befinden sich an verschiedenen Orten;
- Die Kommunikation kann in Echtzeit erfolgen (wie z. B. bei der Nutzung von Chat-Diensten über Apps wie *Skype*® oder *Whatsapp*®) oder zeitversetzt (wie beim Austausch von E-Mails oder Online-Formularen, wenn ein gewisser zeitlicher Abstand zwischen der Kommunikation es Opfers und der Antwort der Fachkraft liegt).

Trotz der dürftigen Belege für die Effektivität von Online-Unterstützung, besonders im Hinblick auf Cyberkriminalitätsopfer, konnten einige Vorteile festgestellt werden.

HIGHLIGHT | DATEN IM FOKUS:

Im Rahmen des *T@LK Project – Online-Unterstützung für Kriminalitätsopfer*, das vom Gerechtigkeitsprogramm der Europäischen Union finanziert wird, wurde unter 60 Organisationen und Opferhilfsdiensten in Europa eine Umfrage über Online-Unterstützung und remote Unterstützung für Kriminalitätsopfer durchgeführt. Unter anderem wurde nach den Vorteilen gefragt, die Online-Unterstützung für Kriminalitätsopfer mit sich bringt:

- 82 % der teilnehmenden Organisationen nannten *Zugänglichkeit* als einen Vorteil.
- Etwa 80 % der teilnehmenden Organisationen, die selbst Online-Unterstützung anbieten, nannten *Bequemlichkeit* und *Flexibilität* bei der Zugänglichkeit als Vorteile. Bei den Organisationen, die über kein Online-Unterstützungsangebot verfügten, war dieser Anteil geringer (58 %).
- 60 % der Organisationen mit Online-Angebot sahen *vereinfachten Zugang* als Vorteil, besonders für Opfer, für die herkömmliche Unterstützungsangebote schwer erreichbar sind. Bei den Organisationen ohne Online-Angebot lag der Anteil bei 74 %.
- Die *Erleichterung der ersten Kontaktaufnahme mit Hilfsorganisationen und -diensten* wurde von 71 % der Organisationen mit eigenem Online-Angebot als Vorteil genannt, aber nur von 42 % der

Organisationen ohne eigenem Online-Angebot für Kriminalitätsopfer.

- Lediglich 57 % der teilnehmenden Organisationen mit eigenem Online-Angebot sahen eine *größere Anzahl an Opfern, die Zugang zu Unterstützung haben* als Vorteil, während sogar 79 % der Organisationen ohne eigenem Online-Angebot dies als Vorteil nannten.

Der vollständige Bericht mit detaillierten Informationen über diese und weitere Umfrageergebnisse ist abrufbar unter: https://www.apav.pt/publiproj/images/yootheme/PDF/TALK.pdf

HIGHLIGHT | ANGEBOTE IM FOKUS:

Im Rahmen des gleichen Projekts wurde das *T@LK Handbuch - Online-Unterstützung für Kriminalitätsopfer* entwickelt. Dieses Handbuch wurde speziell für Opferhilfsorganisationen erstellt und soll ihnen helfen, Online-Unterstützung zu verstehen und Online-Hilfsangebote für Kriminalitätsopfer einzurichten.

Es ist abrufbar unter https://www.apav.pt/publiproj/images/yootheme/PDF/Handbook_TALK.pdf

3.5. Betreuung von Cyberkriminalitätsopfern durch Fachkräfte

Im Anschluss an die Intervention, besonders eine Krisenintervention, und unter Berücksichtigung der Informationen des Cyberkriminalitätsopfers und als notwendig festgestellten Unterstützungs- und Schutzmaßnahmen, muss das Opfer ggf. (intern oder extern) an einen spezialisierten Betreuungsdienst verwiesen werden, zum Beispiel wenn eine rechtliche, psychologische oder soziale Beratung erforderlich ist, um die Beeinträchtigung des Opfers zu minimieren, die Kontrolle über sein oder Leben zurückzuerlangen oder seine oder ihre Bedürfnisse zu erfüllen.

3.5.1. Rechtsberatung: Ziele und zentrale Aspekte

Rechtsberatung für Cyberkriminalitätsopfer darf ausschließlich von entsprechenden Fachkräften durchgeführt werden. Trotzdem sollte jede Betreuungsfachkraft die geltenden Gesetze sowie weitere lokale und internationale Rechtsbehelfe kennen, die in der jeweiligen Situation eine Rolle spielen. Zu diesem Zweck empfehlen wir die Lektüre bzw. das Nachschlagen in Kapitel 2, Teil I dieses Handbuchs über die gesetzlichen Rahmenbedin-gungen hinsichtlich Cyberkriminalität.

Die Betreuungsfachkraft muss außerdem die verschiedenen Phasen des Strafverfahrens kennen und wissen, in welchem Ausmaß sie das Opfer in jeder Phase unterstützen und informieren kann.

Rechtsberatung umfasst alle Informationen und Aufgaben, die die Fachkraft vor, während und nach den Phasen des Verfahrens für die Begleitung und Unterstützung des Kriminalitätsopfers leisten muss.

Rechtliche Beratung beinhaltet:

- Informationen über die Formen von Cyberkriminalität und die jeweiligen gesetzlichen Rahmenbedingungen;
- Aufklärung und Beratung über die Rechte von Kriminalitätsopfern;
- Unterstützung bei der Analyse von Benachrichtigungen des Gerichts und der Erstellung der Antworten auf diese;
- Unterstützung beim Antrag auf Erstattung der Kosten, die im Rahmen der Teilnahme am Verfahren entstanden;
- Unterstützung bei der Formulierung einer Begründung, warum eine Teilnahme an gerichtlich angeforderten Terminen nicht möglich war;
- Unterstützung beim Verfassen bzw. Erstatten einer Anzeige/einer Meldung;
- Unterstützung/Begleitung durch die Fachkraft bei der Erstattung einer Anzeige/Meldung;
- Unterstützung bei der Formulierung und Einreichung einer Zivilklage (wenn das Opfer dies übernimmt, statt einem Anwalt);
- Unterstützung bei der Beantragung von Schutzmaßnahmen.

3.5.1.1. Die Rechte der Opfer von Straftaten

Die Unterstützung eines Kriminalitätsopfer muss zu jedem Zeitpunkt des Verfahrens sicherstellen, dass das Opfer **effektiv teilnehmen** und **von seinen oder ihren Rechten auf informierte Weise Gebrauch machen kann**.

Die Implementierung der Richtlinie 2012/29/EU des Europäischen Parlaments und des Rates vom 25. Oktober 2012 über Mindeststandards für die Rechte, die Unterstützung und den Schutz von Opfern von Straftaten in die nationale Gesetzgebung soll die Position der Opfer stärken und ihnen Unterstützung und Schutz im Umgang mit dem Justizsystem ermöglichen. Sie betont außerdem die Pflicht des Staates, Kriminalitätsopfer und ihre Verwandten und Freunde vor sekundärer oder erneuter Viktimisierung, Einschüchterung und/oder Vergeltung zu schützen. Die Richtlinie stärkt außerdem die Rolle der Opferhilfsorganisationen bei der Sicherstellung des Zugangs zu qualifizierter, kostenloser und vertraulicher Unterstützung oder als Katalysator für die effektive und informierte Ausübung der Rechte der Opfer von Straftaten, und zwar entweder in ihrer ergänzenden Rolle oder in Vertretung des Staates.

Dieses Handbuchersetzt nicht die Notwendigkeit, die Richtlinie in Gänze[95] zu lesen, sondern hebt hervor, wie wichtig umfassendes Wissen über die vielfältigen Rechte ist, die aus dieser Richtlinie hervorgehen.

Im Folgenden fassen wir einige dieser Rechte zusammen und betonen erneut, dass die Richtlinie und die beratenden Informationen zu ihrer Umsetzung unbedingt unter dem folgenden Link gelesen werden müssen: http://www.infovictims.com/com/

[95] Das vollständige Dokument ist abrufbar unter: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32012L0029.

Das Recht auf Information
Das Recht auf Information ist grundlegend, da es dem Opfer ermöglicht, fundiert am strafrechtlichen Prozess teilzunehmen und von seinen oder ihren Rechten Gebrauch zu machen. Kriminalitätsopfer haben das Recht, über ihre Rechte informiert zu werden, besonders wenn sie zum ersten Mal Kontakt zu Polizei- oder Justizbehörden haben:

- Welche Art von Unterstützung kann das Opfer erhalten und von wem;
- Wie und wo kann eine Straftat gemeldet oder angezeigt werden;
- Wie und unter welchen Umständen kann das Opfer Schutzmaßnahmen einfordern;
- Wo erhält das Opfer Rechtsberatung oder Prozesskostenhilfe;
- Wie und unter welchen Umständen kann das Opfer Schadensersatz vom Täter fordern;
- Wie und unter welchen Umständen kann das Opfer Schadensersatz vom Staat fordern;
- Wie erhält das Opfer Zugang zu Dolmetsch- und Übersetzungsdienstleistungen, wenn er oder sie die Sprache des Verfahrens nicht spricht oder von einer Behinderung beeinträchtigt ist;
- Über welche Verfahren kann das Opfer seine Rechte in dem Mitgliedsstaat ausüben, in dem das Verbrechen stattfand, wenn er oder sie dort nicht ansässig ist;
- Wo kann sich das Opfer beschweren, wenn die Behörden seine oder ihre Rechte nicht anerkennen;
- Wer ist der Ansprechpartner des Opfers, wenn dieses Informationen über den Prozess einfordern oder neue Informationen zur Verfügung stellen möchte;
- Welche Möglichkeiten zur Schlichtung stehen zur Verfügung;
- Wie und unter welchen Umständen kann das Opfer eine Erstattung der Kosten einfordern, die durch seine oder ihre Teilnahme am Verfahren entstanden sind.

Recht auf Bestätigung der Anzeige
Ein Opfer, dass eine Straftat meldet oder bei der zuständigen Behörde Anzeige erstattet, hat Anspruch auf den Erhalt einer schriftlichen Bestätigung.

Das Recht auf Übersetzung
Sämtliche Dokumente und Verordnungen, die Teil des Verfahrens sind, müssen in der Sprache des Landes verfasst sein, in dem das Verfahren stattfindet. Das Recht an einem Strafverfahren mündlich und/oder schriftlich in einer Sprache teilzunehmen, die das Opfer versteht, wird in der Richtlinie gewährt und steht entsprechend jedem Opfer in jedem Mitgliedsstaat zu. Die für ein Strafverfahren zuständige Behörde ist daher verpflichtet, einen Dolmetscher oder Übersetzer zu engagieren, der sowohl die Verfahrenssprache als auch die Sprache des Opfers versteht. Unabhängig von seiner Rolle im Verfahren hat das Opfer das Recht, Übersetzungen aller Informationen über das Verfahren, die er oder sie zur Ausübung seiner oder ihrer Rechte benötigt, in eine Sprache zu erhalten, die er oder sie versteht. Ist das Opfer durch eine Behinderung eingeschränkt, hat er oder sie Anspruch auf Verdolmetschung in einer Form, die ihm oder ihr erlaubt, effektiv am Verfahren teilzunehmen. Dabei kann es sich zum Beispiel um einen Gebärdensprachdolmetscher oder schriftliche Antworten auf mündliche Fragen handeln.

Recht auf Zugang zu Opferunterstützung
Das Opfer hat Anspruch auf kostenlosen und vertraulichen Zugang zu Opferunterstützung, auch wenn das Opfer die Straftat nicht meldet oder Anzeige erstattet.

Anspruch auf rechtliches Gehör
Während des Verfahrens hat das Opfer das Recht, gehört zu werden, für die Untersuchung wichtige Informationen einzubringen und Beweismittel vorzulegen. Allerdings muss das Opfer bei der Meldung oder Erstattung der Anzeige der zuständigen Behörde so viele Informationen und relevante Beweise vorlegen wie möglich. Das Opfer kann während der Untersuchung, zum Beispiel bei der Befragung durch den Staatsanwalt, noch weitere Informationen angeben. Wird der Täter angeklagt (Angeklagter) und der Fall geht vor Gericht, kann das Opfer zusätzliche oder fehlende Informationen hinzufügen und Fragen der verschiedenen involvierten Parteien beantworten.

Aufgrund der besonderen Verletzlichkeit des Opfers kann deren oder dessen Aussage auch während der Untersuchung aufgezeichnet und im späteren Verlauf des Prozesses wieder verwendet werden, um eine erneute Aussage des Opfers zu vermeiden.

Rechte bei Verzicht auf Strafverfolgung
Liegen dem Staatsanwalt gegen Ende des Ermittlungsverfahrens keine ausreichenden Beweise für eine Anklage vor, wird das Verfahren eingestellt. Wurde mehrere Straftaten begangen, wird der Beschuldigte u. U. nur für einige davon angeklagt und andere werden fallen gelassen.

In diesem Fall hat das Opfer das Recht, einen Antrag auf Wiedereröffnung des Verfahrens zu stellen. Das Opfer kann ebenfalls die erneute Untersuchung der Beweismittel oder die Fortsetzung des Ermittlungsverfahrens beantragen, für das er oder sie neue Beweise einreichen kann.

Recht auf Mediation
Bei Straftaten von geringer oder mittlerer Schwere, wie Bedrohung, leichte Körperverletzung, Tätlichkeiten oder anderen, ermöglicht das Gesetz die Beilegung des Falls durch eine Einigung zwischen dem Opfer und dem Beschuldigen, sofern der Beschuldigte geständig ist.

Der Mediationsprozess muss kostenfrei, vertraulich und freiwillig sein, d. h. das Opfer kann jederzeit teilnehmen oder die Teilnahme verweigern.

Ein Mediationsprozess soll eine von einem unparteiischen Vermittler geleitete Kommunikationsmöglichkeit bieten, in deren Rahmen das Opfer von den Auswirkungen und/oder Schäden durch die Tat berichten und der Beschuldigte Verantwortung für die Tat übernehmen kann.

Der Vermittler ist eine speziell ausgebildete Fachkraft, deren Aufgabe die Erleichterung der Kommunikation zwischen den Teilnehmern ist.

Anspruch auf Information oder Prozesskostenhilfe
Das Rechtssystem ist so aufgebaut, dass jeder ohne Einschränkungen seine Rechte ausüben und gerichtlichen Beistand einfordern kann sowie Zugang zu allen Gesetzen und Gerichten hat, unabhängig von kulturellen oder sozialen Umständen, unzureichenden Mitteln oder Kenntnissen.

Entsprechend hat das Opfer Anspruch auf Rechtsberatung hinsichtlich seiner oder ihrer Rolle im Verfahren. Ist das Opfer am Verfahren beteiligt oder wünscht das Opfer einen Rechtsbeistand, hat aber nicht die finanziellen Mittel dafür, hat er oder sie Anspruch auf Prozesskostenhilfe. Diese kann beinhalten: vollständiger oder teilweiser Erlass der Gebühren; Bestimmung und Zahlung eines Anwalts; Ratenzahlung der Gebühren oder Anwaltskosten.

Anspruch auf Entschädigung für die Teilnahme am Prozess und Kostenerstattung
Jedes Opfer, das an einem Strafverfahren teilnimmt, hat Anspruch auf Entschädigung für die Zeit der Teilnahme und die Erstattung der entstandenen Kosten.

Recht auf Rückgabe von Vermögenswerten
Wurden Objekte oder andere Vermögenswerte aus dem Besitz des Opfers von den zuständigen Behörden als Beweismittel konfisziert und sind nicht länger für das Verfahren notwendig, müssen sie ohne Verzögerung zurückgegeben werden. Die Rückgabe muss so schnell wie möglich erfolgen, damit das Opfer nicht länger als unbedingt notwendig aufgrund eines Strafverfahrens auf seinen oder ihren Besitz verzichten muss.

Recht auf Entschädigung
Jeder, der als Folge einer Straftat einen Schaden erleidet, hat Anspruch auf Entschädigung.

Der Täter ist verpflichtet, die Entschädigung zu leisten. Sollte die Straftat das Opfer in finanzielle Not bringen oder der Täter nicht in der Lage sein, das Opfer im vorgesehenen Zeitrahmen zu entschädigen, kann ein Antrag auf eine Vorauszahlung durch den Staat gestellt werden.

Schutzanspruch
Opfer und ihre Verwandten haben Anspruch auf Schutz vor Vergeltungstaten, Einschüchterung oder eine Fortsetzung der kriminellen Handlungen gegen sie. Sie haben das Recht bei ihrer Aussage vor jeglichen Handlungen geschützt zu werden, die ihr Leben, körperliche Unversehrtheit, emotionales und psychisches Wohlbefinden und Würde beeinträchtigen könnten.

Gehen die Behörden von einer ernsthaften Bedrohung durch Rache aus oder liegen belastbare Beweise vor, dass die Sicherheit und Privatsphäre des Opfers absichtlich und schwer verletzt werden könnte, müssen angemessene Sicherheitsmaßnahmen für das Opfer, seine oder ihre Familie oder andere nahestehende Personen eingeleitet werden.

Schutz und Sicherheit des Opfers können während dem Verlauf des Verfahrens durch freiheitsbeschränkende Zwangsmaßnahmen gegen den oder die Beschuldigten gewährleistet

werden, sofern die Gefahr für Flucht, Verschleierung von Beweisen oder Fortsetzung der kriminellen Aktivitäten oder eine Gefahr für die Öffentlichkeit besteht.

Sind Leben, körperliche und geistige Unversehrtheit, Freiheit oder Vermögen des Opfers oder anderer Zeugen durch deren Beitrag zur Untersuchung und Verfolgung einer Straftat bedroht, können sie Schutzmaßnahmen beantragen.

Ansprüche der Opfer mit besonderen Schutzbedürfnissen
Ein Opfer mit besonderen Schutzbedürfnissen ist eine Person, die aufgrund ihrer persönlichen Merkmale oder der Art der erfahrenen Straftat und/oder deren Umstände besonders anfällig für weitere Viktimisierung, sekundäre Viktimisierung, Einschüchterung oder Vergeltung ist und daher besondere Betreuung und vor allem Schutz benötigt.

Diese Anfälligkeit muss in jedem Fall individuell festgestellt werden, tritt aber besonders wahrscheinlich bei Opfern auf, die aufgrund der Schwere der Tat erheblichen Schaden erlitten haben, die aufgrund ihrer persönlichen Merkmale diskriminiert wurden oder die durch ihre Beziehung zum und Abhängigkeit vom Täter besonders anfällig sind.

Entsprechend benötigen Opfer von terroristischen Akten, organisierter Kriminalität, Menschenhandel, geschlechterspezifischer Gewalt, Gewalt in intimen Beziehungen, sexueller Gewalt oder Hassverbrechen besondere Aufmerksamkeit. Unabhängig von der Art der Straftat müssen Kinder, ältere Menschen, kranke oder behinderte Menschen bei der Feststellung der Anfälligkeit gesondert betrachtet werden.

Das Recht auf Vergessenwerden[96]
Dieses Recht garantiert dem Inhaber personenbezogener Daten, dass er oder sie die Löschung seiner oder ihrer personenbezogenen Daten jederzeit mündlich oder schriftlich vom Datenverantwortlichen einfordern kann. Dieses Recht kann ausgeübt werden, wenn personenbezogene Daten als ungeeignet oder irrelevant angesehen werden oder ihre Relevanz verloren haben.

3.5.1.2. Die Wichtigkeit der Speicherung digitaler Beweise

„Die Beweise belegen die Richtigkeit der Fakten" (Artikel 341 des portugiesischen Zivilgesetzbuchs) und „das Beweismittel betrifft *alle Fakten, die für die rechtliche Existenz oder Nicht-Existenz der Straftat, die Bestrafung oder Nicht-Bestrafung des Beschuldigten, die Erlassung eines Haftbefehls und die Feststellung einer angemessenen Freiheitsstrafe relevant sind"* (Artikel 124 (1) der portugiesischen Strafprozessordnung). Im Fall einer Zivilklage sind *Beweismittel* die Fakten, die für die Feststellung der Haftung notwendig sind (Artikel 124 (1) und (2) der portugiesischen Strafprozessordnung). Gemäß Artikel 125 der portugiesischen Strafprozessordnung sind im portugiesischen Rechtssystem alle *„Beweismittel zulässig, die nicht verboten sind"*.

[96] Im Gegensatz zu den o. g. Rechten ist dieses nicht Bestandteil der Richtlinie 2012/29/EU. Es ist in Artikel 17 der Datenschutz-Grundverordnung festgeschrieben. Weitere Informationen dazu finden Sie in Teil I, Kapitel 2, Ab-schnitt 2.2 dieses Handbuchs.

3. BETREUUNG VON CYBERKRIMINALITÄTSOPFERN

Die Untersuchung von Straftaten, die im digitalen Raum erfolgen, birgt einige Hindernisse (Martellozzo & Jane, 2017). Studien und Forscher, die sich mit der Analyse von Cyberkriminalität und den Schwierigkeiten bei der **Meldung/Anzeige**[97] **und Untersuchung von Cyberkriminalität** beschäftigen, identifizieren unter anderem die folgenden Hindernisse:

- Der „Ort", an dem die kriminelle Tat stattfand;
- Die Identifizierung des Täters (besonders im Hinblick auf die Anonymität der Cyberspace-Umgebung und der Flüchtigkeit der Beweise für ihre Taten, die einfach blockiert, modifiziert, unbrauchbar gemacht oder gelöscht werden können);
- Die Herstellung von Kausalität in Fällen, die häufig mehrere Täter und Opfer betreffen.

Die Schwierigkeiten bei der Untersuchung werden von den Eigenschaften der Cyberkriminalität verursacht: Transnationalität, Anonymität und Variabilität (ständige Veränderung und permanente Entwicklung neuer Formen) (Santos, 2016; Holt & Bossler, 2015).

HIGHLIGHT | ANGEBOTE IM FOKUS:

Das Projekt *SIRIUS* unter der Leitung des *Europäischen Zentrums für Terrorismusbekämpfung von Europol* und dem *Europäischen Zentrums zur Bekämpfung der Cyberkriminalität*, in Zusammenarbeit mit *Eurojust* und dem *Europäischen Justiziellen Netz*, soll Behörden beim Umgang mit der Komplexität und Informationsflut in der sich schnell verändernden Online-Welt unterstützen.

Das Projekt organisiert Wissensvermittlung durch Veranstaltungen und eine zugangsbeschränkte Plattform, auf der Mitgliedsstaaten (und Drittstaaten, die ein operatives Abkommen mit EUROPOL geschlossen haben) Zugang zu aktuellen Informationen und digitalen Beweisen für Ermittlungsverfahren haben.

Weitere Informationen sind abrufbar unter: www.europol.europa.eu/sirius

Die Verwendung von IKT für kriminelle Zwecke steigert die Bedeutung digitaler Beweise (Balkin et al., 2007).

Einer der größten Unterschiede zwischen Cyberkriminalität und *herkömmlichen Formen der* Kriminalität ist die Natur der Beweise. Es gibt Unterschiede in der Form der Beweise und der Speicherung, sie stammen von verschiedenen Orten und werden auf verschiedene Weise ermittelt. Des Weiteren sind digitale Beweismittel immateriell und allgemein anfällig und sie können in massiven Mengen auftreten, was zu grundlegenden logistischen Herausforderungen führt (Grabosky, 2007).

Da digitale Beweismittel hoch anfällig und temporärer Natur sind, treten zusätzliche Schwierigkeiten bei der Prüfung ihrer Echtheit und der Sicherung relevanter Merkmale auf. Diese sind aber erforderlich, um sicherzustellen, dass die Beweise zulässig, authentisch, korrekt und vollständig sind (Marques, 2013). Eine einzige Abweichung bei der Speicherung von Beweismitteln und der daraus

[97] Siehe zu diesem Zweck Teil I, Abschnitt 1.4 dieses Handbuchs, welcher die Differenz zwischen der Anzahl gemeldeter und der Anzahl tatsächlich begangener Straftaten im Zusammenhang mit Cyberkriminalität sowie die Gründe für nicht erfolgte Meldungen erörtert.

folgende Bruch der Beweiskette kann die Beweise rechtlich unzulässig machen (*idem*).

Wie andere Beweisarten müssen digitale Beweismittel für den Erhalt ihrer Beweiskraft verändert werden, nicht nur hinsichtlich ihrer physischen Integrität, sondern auch der enthaltenen Daten. Abhängig vom Gerät müssen spezielle Maßnahmen für Aufnahme, Verpackung, Transport und Speicherung ergriffen werden (*idem*).

3.5.1.3. Die Bedeutung interinstitutioneller Zusammenarbeit

Aufgrund der Natur des Kontakts zu Cyberkriminalitätsopfern und der Erfüllung ihrer festgestellten Unterstützungsbedürfnisse, die oft im Zusammenhang mit dem Verfahren stehen, muss eine **institutionsübergreifende Zusammenarbeit zwischen den Opferhilfsorganisationen und -diensten und den Polizei- und Justizbehörden** in Betracht gezogen werden.

Idealerweise erfolgt diese institutionsübergreifende Zusammenarbeit über formale Partnerschaften in Form von **Protokollen und Kooperationsvereinbarungen**, die gemeinsame Abläufe und Verfahren festlegen, um die Kommunikation und Weitergabe von Informationen zu vereinfachen und so zu einer besseren Unterstützung, Behandlung und Intervention für die Kriminalitätsopfer im Allgemeinen und Cyberkriminalitätsopfer im Besonderen führen.

HIGHLIGHT | ANGEBOTE IM FOKUS:

Die portugiesische Opferhilfsorganisation (APAV – Associação Portuguesa de Apoio à Vítima) und die portugiesische Bundespolizei (Polícia Judiciária), die für die Untersuchung von Cyberkriminalität zuständig ist, unterzeichneten 2019 eine Kooperationsvereinbarung für ihre Zusammenarbeit im Internet der *Linha Internet Segura*.

Dabei handelt es sich um ein von der APAV betriebenes Telefon- und Online-Hilfsangebot des Zentrums für Internetsicherheit mit zwei Komponenten: Beratung und Aufklärung hinsichtlich Problemen bei der Internet- und IKT-Nutzung sowie Unterstützung und Aufklärung bei Cyber-Verbrechen (Helpline), Meldung illegaler Inhalte im Internet (Hotline).

Diese Kooperationsvereinbarung umfasst auch die Einrichtung eines Empfehlungssystems für Cyberkriminalitätsopfer, deren Fälle von der Polícia Judiciária bearbeitet werden, an die APAV und erlaubt die effektive Weitergabe von Informationen über Cyberkriminalität an die Polícia Judiciária, die über die Helpline und Hotline erhalten werden.

Allgemein dienen diese Vereinbarungen und Protokolle der Einrichtung und Umsetzung von **Mechanismen für die Weiterempfehlung von Cyberkriminalitätsopfern**, wie auch im o. g. Beispiel.

In dieser Hinsicht rät die o. g. Richtlinie 2012/29/EU, dass die Weiterempfehlung der Cyberkriminalitätsopfer an Opferhilfsorganisationen durch zuständige Behörden vereinfacht wird, um sicherzustellen, dass das Opfer **gemäß seiner oder ihrer Rechte vor, während und für einen**

angemessenen Zeitraum nach dem Abschluss des Prozesses Zugang zu Unterstützung hat.

Davon ausgehend ist der **Empfehlungsprozess** ein **Mechanismus institutionsübergreifender Zusammenarbeit**, bei dem eine Organisation Informationen über das Auftreten von Straftaten und ihre Opfer mit der Einwilligung des Opfers und zum Zweck der angemessenen Unterstützung des Opfers an eine andere Organisation weitergibt. Eine Empfehlung basiert auf einem proaktiven Prozess, der ein wesentlicher Bestandteil der Unterstützungsmaßnahmen für Kriminalitätsopfer durch einen Dienst oder eine Hilfsorganisation ist. Eine Empfehlung muss jederzeit dem Willen des Opfers entsprechen, seine oder ihre Zustimmung haben und seinen oder ihren Zugang zu besser für die Erfüllung seiner oder ihrer Bedürfnisse geeigneter Betreuung zum Zweck haben.

HIGHLIGHT | WICHTIGSTE INFORMATION:

Die Art und Weise, wie Informationen über Kriminalitätsopfer gesammelt und übertragen werden, muss ebenfalls festgelegt und von den Organisationen vereinbart werden, die Teil eines speziellen Empfehlungsmechanismus sind.

Unabhängig von der Methode, mit der Informationen gesammelt und übertragen werden, muss sichergestellt sein, dass die weitergegebenen Informationen die Identifizierung des Opfers und Verständnis der Viktimisierungssituation ermöglichen. Das Risiko, dass das Opfer erneut über die Situation berichten muss, die zur Kontaktaufnahme mit der Hilfsorganisation oder dem Dienst geführt haben, ist zu reduzieren.

Die folgenden Hintergrundinformationen sollten daher Bestandteil jeder Empfehlung sein:

- Victim's name;
- Victim's contact and preferred time for contact;
- Brief description of the crime/situation of victimisation (type of crime; relationship to offender, where applicable; consequences and impact of victimisation);
- Observations and support provided by the organisation (e.g. psychological support, legal information and other observations relevant to the organisation to which the victim was referred).

HIGHLIGHT | ANGEBOTE IM FOKUS:

Projekt VICToRIIA – Bewährte Methoden bei der Opferunterstützung Empfehlungen, Aufklärung, individuelle Beurteilung wird vom Litauischen Zentrum für Kriminalitätsprävention (NPLC) gefördert und vom Gerechtigkeitsprogramm der Europäischen Union finanziert und soll zur Entwicklung von Empfehlungsmechanismen zwischen Opferhilfsorganisationen und Strafverfolgungsbehörden beitragen. Im Rahmen des Projekts wurde ein Handbuch für die effektive und sichere Weiterempfehlung von Opfern entwickelt.

Neben diversen Handlungsanweisungen für die effektive und sichere Weiterempfehlung von Opfern wird die Wichtigkeit der Gewährleistung der Sicherheit des Opfers und des Schutzes der personenbezogenen Daten des Opfers gemäß der Datenschutz- Grundverordnung der EU (DSGVO) und sämtlicher relevanter, nationaler Gesetze betont.

Weitere Informationen abrufbar unter: http://nplc.lt/victoriia/.

3.5.2. Psychologische Betreuung: Ziele und zentrale Aspekte

Psychologische Betreuung soll für das Opfer und/oder dessen Familie eine therapeutische Erfahrung sein und die negativen Auswirkungen einer schlimmen und potenziell traumatischen Erfahrung minimieren. Sie setzt bei dem Bedürfnis des Opfers und/oder dessen Familie an, das psychische und emotionale Wohlbefinden wiederherzustellen, das von der Viktimisierungserfahrung beeinträchtigt wurde (APAV, 2013b).

Psychologische Betreuung sollte ausschließlich von Fachkräften mit entsprechendem Abschluss in der Psychologie gewährleistet werden, deren Qualifikation und Erfahrung allgemein und gegebenenfalls durch die zuständige Aufsichtsbehörde des Landes, die die Berufsstandards festlegt, anerkannt ist.

Es gibt verschiedene Modelle und Schulen, die in der psychologischen Intervention bei Kriminalitätsopfern Anwendung finden, einschließlich psychodynamischer Therapie, kognitiver Verhaltenstherapie, narrativer und konstruktivistischer Therapie. Ungeachtet der bevorzugten Schule der Fachkraft oder ihrer Organisation ist ein breites Wissen über die verschiedenen Formen der Cyberkriminalität und ihre Dynamiken, die Risikofaktoren für Cyberkriminalität und ihren Einfluss auf das psychische, emotionale und soziale Wohlbefinden des Opfers zwingend erforderlich[98].

Die Hauptziele psychologischer Betreuung sind:

- Linderung und Reduzierung der Symptome;
- Reduzierung von Unwohlsein und dysfunktionalen Verhaltensweisen;
- Stärkung adaptiver Verteidigungsmechanismen;
- Verbesserung der Anpassung an die Umgebung;
- Verbesserung des Realitätssinns;
- Stärkung des Selbstbewusstseins;
- Stärkung der Autonomie;
- Wiederherstellung der psychischen Ausgeglichenheit.

In den folgenden Abschnitten stellen wir Richtlinien und einige der allgemein wichtigen Aspekte vor, die es bei der psychologischen Betreuung von Cyberkriminalitätsopfern zu berücksichtigen gilt. Die abgedeckten Inhalte sind kein psychologisches Interventionsprogramm für Cyberkriminalitätsopfer, sondern lediglich Annahmen und Prinzipien, die unabhängig von der Schule, der die Fachkraft oder Organisation anhängt, bei jeglichem Interventionsprozess auf dem Gebiet der Cyberkriminalität berücksichtigt werden sollten.

3.5.2.1. Anforderungen an und Arbeitsprinzipien für psychologische Betreuung

Einige **Anforderungen**, die für den Erfolg einer psychologischen Intervention berücksichtigt werden sollten, sind (APAV, 2013b; Alexy et al., 2005):

[98] Siehe Kapitel 1, 3, und 4 in Teil I dieses Handbuchs, in denen die Typologien und verschiedenen Arten der Cyberkriminalität, die sozio-demografischen und aus dem Verhalten erwachsenden Risikofaktoren und die Auswirkungen von Cyberkriminalität erörtert werden.

- Die Fachkraft muss eine therapeutische Allianz und eine unterstützende Beziehung mit dem Opfer eingehen, frei von Stigmatisierung und Vorurteilen;
- Die Fachkraft muss die Auswirkungen der Cyber-Viktimisierungserfahrung gründlich untersuchen, besonders die Anzeichen für schädliche psychische oder emotionale Verhaltensänderungen, einschließlich Rückzug und Flashbacks (Symptome einer posttraumatischen Belastungsstörung), und verändertes Verhalten im sozialen oder beruflichen Kontext, sowie das Suizidrisiko.
- Die Fachkraft sollte auch das mögliche Auftreten von Komorbiditäten[99] mit anderen psychischen Störungen und/oder Erkrankungen überprüfen und das Opfer, falls erforderlich, an andere Fachkräfte und/oder eine spezialisiertere Organisation verweisen.
- Die Fragen müssen zeitlich passend und einfühlsam gestellt werden, um dem Opfer seine oder ihre Aussage zu erleichtern;
- Die Fachkraft sollte die Gefühle, Gedanken und Vorgeschichte der Viktimisierung des Opfers validieren;
- Die Fachkraft hilft dem Opfer beim Umgang mit negativen Gefühlen, wie Angst, Wut, Scham oder Schuld, die aus der Cyber-Viktimisierungserfahrung entstehen;
- Die Fachkraft klärt das Opfer über mögliche Reaktionen auf die Cyber-Viktimisierungserfahrung auf, bestätigt, dass die Gedanken, Gefühle und das Verhalten des Opfers eine normale Reaktion auf unerwartete Erfahrungen sind, und schürt Hoffnung im Hinblick auf den Heilungsprozess;
- Die Fachkraft unterstützt das Opfer bei der Etablierung von Strategien, um kognitives und tatsächliches Rückzugsverhalten zu reduzieren, den effektiven Umgang mit Flashbacks und dem Auftreten negativer Gefühle wie Ineffizienz, Inkompetenz, Hoffnungslosigkeit, Wut, Schuld und Scham zu lernen und ein gestärktes Selbstbewusstsein und den Aufbau von Vertrauensbeziehungen zu fördern.

Die folgenden **Arbeitsprinzipien** sind ebenfalls zu berücksichtigen (APAV, 2011; APAV, 2013b):

Therapievereinbarung
Zu Beginn der Betreuung sollte ein Regelwerk mit dem Opfer vereinbart werden – die *Therapievereinbarung*, die die Uhrzeit, Häufigkeit und Dauer der Sitzungen festlegt, die Regeln für die Teilnahme und Pünktlichkeit sowie Ziele und Pläne für die Betreuung. Diese Vereinbarung soll das Engagement und die Verantwortlichkeit des Opfers für den psychologischen Betreuungsprozess und die daraus resultierenden Erfolge sicherstellen und zu dessen aktiver Einbringung im Interventionsprozess und beim Verfolgen der Ziele beitragen.

Neutralität und Anonymität
Die Fachkraft kommuniziert und interagiert mit dem Opfer frei von persönlicher Meinung, Selbstoffenbarung, Manipulation und anderen, unangemessenen Verhaltensweisen in einer psychologischen Betreuung. Die Fachkraft bestärkt das Opfer darin, sich emotional frei und ehrlich auszudrücken, ohne sich zu schämen.

Neutralität bezeichnet keinen Mangel an Empathie, sondern ist, wie bereits erwähnt, eine wichtige Kompetenz beim Aufbau eines Vertrauensverhältnisses zwischen Opfer und Fachkraft[100].

[99] Komorbidität beschreibt das Auftreten zweier oder mehrerer Störungen, die bei der gleichen Person auftreten.

[100] Weitere Informationen über Kommunikation und Empathie im Kontakt zu Cyberkriminalitäts- und Kriminalitätsopfern finden Sie in Kapitel 2 dieses Teils des Handbuchs.

Privatsphäre und Vertraulichkeit
Das Opfer muss sicher sein können, dass Informationen, die im Rahmen der psychologischen Betreuung preisgegeben werden, diesen Rahmen nie verlassen. Die Weitergabe von Informationen über die psychologische Betreuung an Dritte (Personen oder Organisationen) erfolgt ausschließlich nach vorheriger Zustimmung des Opfers für diesen speziellen Zweck.

3.5.2.2. Phasen des psychologischen Betreuungsprozesses

Anfangsphase | Therapeutische Beziehung und Informationsbeschaffung

Entwicklungsphase | Umsetzung des psychologischen Interventionsplans

Endphase | Prüfung, inwiefern die angestrebten Ziele und Veränderungen erreicht wurden

Anfangsphase des psychologischen Betreuungsprozesses

Diese Phase widmet sich dem **Aufbau eines Vertrauensverhältnisses** zwischen dem Opfer und der Fachkraft, die die psychologische Betreuung übernimmt. Die persönlichen und beruflichen Fertigkeiten der Fachkraft sowie deren empathische Kommunikationskompetenz (siehe Abschnitte 2.1 und 2.2 in Kapitel 2 in Teil I dieses Handbuchs) sind hier ausschlaggebend. In dieser Phase des Betreuungsprozesses wird die Therapievereinbarung eingegangen.

In der Anfangsphase des Interventionsprozesses erfolgen die **Informationsbeschaffung** und Analyse, auf deren Grundlage ein Plan und Strategien für die psychologische Betreuung erstellt werden.

In dieser Hinsicht kann es hilfreich sein, bei (eventuell vorhandenen) anderen Fachkräften, die das Opfer vorher bei der Organisation kontaktiert hat, Informationen über das Cyberkriminalitätsopfer[101] einzuholen. So kann sich die Fachkraft ein umfassendes Bild der Lebensgeschichte, internen und externen Ressourcen und die Cyberkriminalitätserfahrung und deren Auswirkungen machen.

Außerdem kann die Fachkraft **Skripte, Interview und psychologische Beurteilungsmethoden einsetzen**, um die relevanten Informationen für die Erstellung eines Interventionsplans (besonders im Hinblick auf die Anforderungen des Opfers und dessen emotionaler und psychischer Bedürfnisse) zu erhalten und zu sortieren und um spezifische Bereiche psychischer und emotionaler (Dys-) Funktion zu analysieren. Die Informationsbeschaffung vom Opfer sollte durch die Beobachtung ihres Verhaltens und ihrer **non-verbalen Kommunikation und Ausdrucksweise** ergänzt werden, da es sich dabei um wichtige Indikatoren für den emotionalen Zustand, Wohlbefinden und Funktionalität des Opfers handelt.

[101] Weitere Informationen über die Wichtigkeit der Informationsbeschaffung werden in Teil II, Kapitel 2, Abschnitt 2.3 dieses Handbuchs dargelegt.

Die Informationsbeschaffung für die Erstellung eines psychologischen Interventionsplans kann an sich ein therapeutischer Prozess sein. Durch sie kann nicht nur ein Überblick über die von der Cyber-Viktimisierungserfahrung betroffenen (internen und externen) Ressourcen gewonnen werden, sie trägt auch zur freien, emotionalen Ausdrucksfähigkeit des Opfers und die Entwicklung einer Schilderung der Cyber-Viktimisierungserfahrung bei.

Entwicklungsphase des psychologischen Betreuungsprozesses

Diese Phase kennzeichnet sich durch die **Umsetzung des psychologischen Interventionsplans und im Vorfeld festgelegter Strategien** aus und kann mehrere Termine oder Sitzungen in Anspruch nehmen. Es werden weiterhin Informationen gesammelt und analysiert, da sie Bestandteil eines umfassenden, bereichsübergreifenden Interventionsprozesses sind.

Unabhängig von den angewendeten Interventionsstrategien und theoretischen Ansätzen sollte die Fachkraft bei der Umsetzung des psychologischen Umsetzungsplans das Folgende versuchen:

- **Emotionalen Ausdruck und Kommunikation vereinfachen**: Die Fachkraft ermutigt das Opfer, über seine oder ihre Gefühle und Gedanken zu sprechen, beruhigt ihn oder sie und zeigt ihm oder ihr, dass dies ohne Verurteilung geschehen kann;
- **Verständnis des Opfers für seine oder ihre Probleme und Reaktionen fördern**: Die Fachkraft erklärt dem Opfer die Art von Kriminalität, der er oder sie zum Opfer gefallen ist und stellt ähnliche Cyber-Viktimisierungssituationen vor, damit er oder sie sich leichter mit seiner oder ihrer Viktimisierungsgeschichte identifizieren kann, und als Folge davon auch mit den daraus resultierenden Bedürfnissen, Problemen und Lösungsansätzen;
- **Interesse und Empathie zeigen**: siehe Teil II, Kapitel 2, Abschnitte 2.1 und 2.2 dieses Handbuchs zum Thema;
- **Selbstbewusstsein stärken**: Die Stärkung des Selbstbewusstseins des Opfers trägt zur Umsetzung der beabsichtigten Verhaltensänderungen bei.
- **Problemlösung vereinfachen**: Die Fachkraft unterstützt das Opfer Schritt für Schritt dabei, sich Widrigkeiten zu stellen, Entscheidungen zu treffen und Probleme zu lösen.

Endphase des psychologischen Betreuungsprozesses

Der richtige Moment für das Ende eines psychologischen Betreuungsprozesses ist schwierig abzuschätzen, weshalb die Fachkraft zusammen mit dem Opfer die zu Beginn der Intervention im Interventionsplan festgelegten Ziele beurteilen sollte, um:

- Herauszufinden, welche Bedeutung das Opfer seiner oder ihrer Cyber-Viktimisierungserfahrung zuschreibt und in welchem Ausmaß er oder sie die Ziele als ganz oder teilweise erfüllt ansieht;
- Präventions- und Schutzmaßnahmen festzulegen;
- Zu bestätigen, welche Fähigkeiten das Opfer erlernt hat, um die Verbesserungen und

Veränderungen durch den Interventionsprozess aufrechtzuerhalten.

Nach Ende der Betreuung muss die Fachkraft sicherstellen, dass ein **Follow-Up** des Falls durchgeführt wird, damit die gewonnenen Einsichten auch nach Beendigung der Betreuung zur Verfügung stehen.

Unabhängig von der Phase des psychologischen Betreuungsprozesses finden Sie in der folgenden Tabelle einige Kommunikationstechniken, die beim Erreichen der Ziele der Intervention helfen können (APAV, 2013b).

Tabelle 7: Nützliche Kommunikationstechniken und -strategien für den psychologischen Betreuungsprozess

Katharsis - Vereinfachung des Ausdrucks von Gefühlen und Emotionen
Befragung - Informationsbeschaffung durch geschlossene (z. B. „Wie heißen Sie?") und offene (z. B. „Was denken Sie darüber?") Fragen
Restrukturierung - Neuordnung der Informationen des Opfers, um Perspektivwechsel zu erreichen
Fokus - Auswahl der wichtigsten Informationen für die Umsetzung eines Interventionsziels
Interpretation - den Aussagen des Opfers Bedeutung zumessen
Klärung - die Aussagen des Opfers hinterfragen und ggf. klären, um Symptome, Gefühle und Verhaltensweisen besser zu verstehen
Konfrontation - widersprüchliche Informationen gegenüberstellen, um Zweifel oder Widersprüche auszuräumen und/oder das Verhalten bzw. die Aussagen des Opfers auf die Probe zu stellen
Suggestion - Aufbringen einer Idee oder eines Gefühls, um alternative Szenarien einzubringen
Wiederholung - Wiederholung eines Worts oder einer Frage zu Informationen des Opfers als eine Möglichkeit, die Aufmerksamkeit des Opfers während dem Interventionsprozess zu unterstützen und die empathische Kommunikation und Beziehung zwischen dem Opfer und der Fachkraft zu stärken
Stille - hauptsächlich Möglichkeit zur Reflektion
Stärkung des Selbstbewusstseins - Stärkung und Wiederherstellung des Selbstbewusstseins des Opfers durch Zustimmung zu einer Idee, einem Gedanken, einem Verhalten oder einer Entscheidung
Beratung - Vorschlag von Verhaltensweisen oder Entscheidungen, um beim Opfer gesunde Verhaltensweisen wiederherzustellen, Symptome zu reduzieren oder Krisen zu verhindern
Aufklärung - Information über relevante Probleme oder Situationen

3.5.3. Soziale Betreuung: Ziele und zentrale Aspekte

Laut dem Internationalen Zusammenschluss der Profession Sozialer Arbeit (2005 cit. in APAV, 2013b) umfasst die Soziale Arbeit die Förderung gesellschaftlicher Veränderung, Konfliktlösung in zwischenmenschlichen Beziehungen und den Menschen dabei zu helfen, ihr Wohlbefinden

zu steigern. Soziale Arbeit soll also **positive Veränderungen in der psychischen und sozialen Funktionsweise von Personen, Gruppen und Gemeinschaften** bewirken, Anfälligkeiten reduzieren und Möglichkeiten für ein zufriedenstellenderes Sozialleben bieten.

Die Ziele der Sozialen Arbeit sind:

- Förderung der Inklusion anfälliger oder gefährdeter sozialer Gruppen;
- Förderung des Wohlbefindens und der Problemlösung durch Intervention zwischen Personen, in Gruppen und Gemeinschaft;
- Umsetzung von Schutzmaßnahmen für Personen, die aufgrund ihres Zustands oder ihrer Situation selbst nicht dazu in der Lage sind.

Soziale Arbeit umfasst entsprechend verschiedenste Bereiche, wie Bildung, Aufklärung und Betreuung, psychosoziale Unterstützung und Dienst- oder Ausrüstungsmanagement (APAV, 2013b).

Soziale Arbeit unterliegt der Verantwortlichkeit der Sozialarbeiter, Sozialpolitiker und anderer, angemessen qualifizierter Fachkräfte aus der Sozialen Arbeit (idem).

Wie auch bei anderen Formen der spezialisierten Betreuung erfordert die Bereitstellung sozialer Unterstützung für Cyberkriminalitätsopfer, dass die Fachkraft zusätzlich zu ihrer akademischen Ausbildung die theoretischen und konzeptionellen Grundlagen der Bedürfnisse von Cyberkriminalitätsopfern kennt und angemessen handeln kann. Außerdem muss sich die Fachkraft der Charakteristika und Dynamiken der verschiedenen Formen der Cyberkriminalität und deren Auswirkungen auf die Opfer bewusst sein und diese verstehen[102].

3.5.3.1. Von der Sozialen Diagnostik zur individualisierten Intervention

Soziale Diagnostik beschreibt die Erhebung und Ordnung der Informationen über einen Kontext, um dessen Probleme und Anforderungen ebenso wie deren Ursachen und Entwicklung zu verstehen. Mithilfe der sozialen Diagnostik können Prioritäten und Interventionsstrategien **basierend auf den verfügbaren Ressourcen und sozialen Akteuren** entwickelt werden (Ander-Egg & Idánez, 1999 cit *in APAV*, 2018).

Soziale Diagnostik sollte einer der ersten Schritte in der sozialen Unterstützung sein. Sie repräsentiert den fortlaufenden Prozess, die Wahrnehmung der Realität durch eine bestimmte Person, Gruppe oder Gemeinschaft, sowie deren beständige Veränderung, zu verstehen und erfordert dadurch die permanente Sammlung und Analyse von Informationen.

Soziale Diagnostik ist eine Grundlage für die individualisierte Intervention bei Kriminalitäts- und Cyberkriminalitätsopfern. Erst nach der Klärung der Beziehungssituation und der sozialen wie institutionellen Situation des Opfers kann die Fachkraft einen Interventionsplan erstellen,

[102] Siehe Kapitel 1, 3 und 4 in Teil I dieses Handbuchs über die Typologien und verschiedenen Formen der Cyberkriminalität, die Risikofaktoren im Zusammenhang mit Cyberkriminalität, die Folgen und die Bedürfnisse von Cyberkriminalitätsopfern.

der das Opfer, dessen primäres Unterstützungsnetzwerk und die vorhande-nen institutionellen Unterstützungsstrukturen miteinbezieht (García & Romero, 2012 cit *in APAV*, 2018). Dieser Ansatz für die Konzeption individualisierter Intervention wird als Fallmethode bezeichnet.

Die Fallmethode besteht aus vier Grundschritten (*idem*):

- Analyse und Feststellung des Problems;
- Erstellung eines Programms/einer Intervention;
- Umsetzung der Intervention;
- Beurteilung.

Für die Umsetzung dieser vier Schritte, die eine individualisierte, auf die sozialen, institutionellen und Beziehungsbedürfnisse des Opfers abgestimmte Intervention ermöglichen, muss die Fachkraft:

Table II-8: Indivualised intervention and victims needs

Die Umstände der Straftat identifizieren	
Die Identifizierung der Umstände der Straftat und des Opfers erfolgt auf Grundlage der Informationen, die durch den Kontakt zwischen Opfer und Organisation[103] erlangt wurde und umfasst die Cyber-Viktimisierungserfahrung bzw. deren Hintergrund sowie Informationen über das Opfer, dessen Merkmale und gegebenenfalls frühere Viktimisierungserfahrungen.	
Die Bedürfnisse des Opfers feststellen	
Die Feststellung der Bedürfnisse des Opfers erfolgt auf Basis seiner oder ihrer Interessen und unter Berücksichtigung seiner oder ihrer Lebensumstände und der Probleme, die sich aus dem konkreten Fall ergeben. Die Fachkraft muss: • dem Opfer ermöglichen, auszudrücken, was er oder sie braucht oder will; • die ausgedrückten Bedürfnisse klären und wiederholen, um sicherzustellen, dass sie korrekt verstanden wurden; • permanent über bestehende Rechte, Ressourcen und Hilfsangebote aufklären, die dem Opfer helfen, die eigenen Bedürfnisse zu erkennen; • permanent die verschiedenen Bedürfnisse und ihre Dringlichkeit beurteilen, um auf das wichtigste rea-gieren zu können. Dringende Bedürfnisse sind: Sicherheit, Grundbedürfnisse, medizinische und/oder psychologische Betreuung, Obdach und rechtliche Unterstützung. Mittel- und/oder langfristige Bedürfnisse können sein: finanzielle Unterstützung, Unterstützung bei der Ausbildung, Unterstützung bei der (Re-) Integration, Weiterbildung und berufliche Integration. Soziale Unterstützung besteht aus den folgenden vier Dimensionen:	
OBDACH	Cyber-Verbrechen über das Internet und IKT, die im Beziehungskontext geschehen, wie Cyberstalking oder die unerlaubte Veröffentlichung von Bildern und Videos in von Gewalt betroffenen, intimen Beziehungen, können dazu führen, dass das Opfer entweder geplant oder dringend/im Notfall einer Unterkunft bedarf. Die Fachkraft muss die Situation analysieren (das primäre Unterstützungsnetzwerk aus Freunden, Verwandten oder anderen Vertrauenspersonen oder den Bedarf an einem sekundären Unterstützungsnetzwerk identifizieren) das Risiko beurteilen. Erfüllt das primäre Unterstützungsnetzwerk

[103] Siehe Teil II, Kapitel 2, Abschnitt 2.3 dieses Handbuchs.

die erforderlichen Sicherheitsbedingungen, kann die Betreuung dort erfolgen. Sie kann aber auch von Institutionen bereitgestellt werden. In diesem Fall muss die Fachkraft die regionalen und überregionalen Unterbringungsmöglichkeiten kennen und das Opfer entsprechend an Notfall-Hotlines, Notunterkünfte/Einrichtungen, Nichtregierungsorganisationen, Sozialdienste und andere verfügbare Angebote verweisen.

LEBENSMITTEL

Das Cyberkriminalitätsopfer kann, zum Beispiel durch Internetbetrug, in eine ökonomisch schwierige Lage geraten, in der er oder sie nicht in der Lage ist, Grundbedürfnisse wie Lebensmittel oder Medikamente für bestehende Erkrankungen zu erfüllen.

Die Fachkraft braucht einen Überblick über die verschiedenen Organisationen, die in diesem Bereich tätig sind, ihre Ziele, Abläufe und Regeln, um das Opfer angemessen verweisen zu können und beim Kontakt zu diesen Organisationen zu unterstützen.

Zu diesem Zweck muss die Fachkraft die Organisationen im eigenen Land kennen, die für die Erfüllung dieser Bedürfnisse herangezogen werden können, und Opfer gegebenenfalls an Nichtregierungsorganisationen, Sozialdienste, kirchliche Einrichtungen oder andere verfügbare Angebote verweisen.

GESUNDHEIT

Eine Cyber-Viktimisierungserfahrung kann zu körperlichen oder psychischen Erkrankungen führen. Die Fachkraft muss in der Lage sein, passende Organisationen oder Hilfsangebote im Land auszuwählen und das Opfer gegebenenfalls an Notfall-Hotlines, staatlich geförderte Gesundheitsdienste, Nichtregierungsorganisationen, kirchliche Einrichtungen oder andere Gesundheitsdienstleister (einschließlich private Anbieter) zu verweisen.

BERUFLICHE SITUATION

Angesichts der potenziellen Auswirkungen von Cyberkriminalität auf die berufliche Situation des Opfers müssen unter Umständen neue Wege gefunden werden, um den Lebensunterhalt des Opfers sicherzustellen. (Re-) Integration in den Beruf ist unabdingbar für mehr Autonomie. Die Fachkraft muss akademische Qualifikationen, Berufserfahrung, berufliche Interessen und potenziellen Weiterbildungsbedarf des Opfers beurteilen. Die Fachkraft muss das Opfer an zuständige Einrichtungen wie das Jobcenter oder Weiterbildungseinrichtungen verweisen, die ihn oder sie bei der Wiedereingliederung in den Beruf unterstützen. Das Opfer sollte bei der Kontaktaufnahme zu Unternehmen, die zum Profil des Opfers, seiner oder ihrer Fähigkeiten und beruflichen Interessen passen, durch die Fachkraft unterstützt werden.

BILDUNG/AUSBILDUNG

Bestimmte Formen der Cyberkriminalität, wie Cybermobbing, sexueller Missbrauch oder sexuelle Ausbeutung von Kindern im Internet, beeinträchtigen die schulische Situation von Kindern oder Heranwachsenden. In einigen Fällen geschieht dies auch, wenn ein Erziehungsberechtigter Cyberkriminalität zum Opfer fällt. Es ist daher wichtig, dass sich die Fachkraft mit der Schule oder Bildungseinrichtung in Verbindung setzt, um die direkten und indirekten Bedürfnisse des Opfers in diesem Bereich ermitteln und erfüllen zu können. Dies kann zum Beispiel der Wechsel an eine andere Schule oder in ein anderes Ausbildungsprogramm sein, welche zum Schutz der direkten und indirekten Opfer stets diskret erfolgen muss.

Empfehlung und Zusammenarbeit

Diese Grundbedürfnisse (und deren Erfüllung) sind wichtige Bestandteile der Interventionsmaßnahmen im Bereich sozialer Untertützung.

Abhängig von den ermittelten Bedürfnissen und dem Angebot der Organisation, bei der die Fachkraft tätig ist, kann es erforderlich sein, das Opfer an eine andere Stelle zu verweisen und mit anderen Organisationen/Diensten in der Gemeinde zusammenzuarbeiten. Die Fachkraft (und die Organisation, für die sie tätig ist) benötigt für jeden Fachbereich ein sekundäres Unterstützungsnetzwerk auf regionaler und nationaler Ebene, das für die Unterstützung von Kriminalitätsopfern herangezogen werden kann.

Um die Bedürfnisse des Opfers angemessen erfüllen und die beste Betreuung anbieten zu können, kann eine Zusammenarbeit mit Institutionen aus anderen Bereichen erforderlich sein, besonders:

- Sozialdienste (staatliche Einrichtungen, private Stiftungen/Nichtregierungsorganisationen);
- Arbeitsplatz und Arbeitsagentur (einschließlich Jobcenter und berufliche Bildungszentren);

- Personalabteilungen von Unternehmen und anderen regionalen Organisationen oder Ausschüssen;
- Gesundheitsdienste (wie Krankenhäuser, Ärztezentren und Einrichtungen für psychologische Betreuung);
- Bildungs- und/oder Ausbildungsinstitutionen;
- Lokale Behörden (z. B. Gemeinderat oder Pfarrgemeinderat);
- Justizbehörden (Polizei, Gerichte, forensische Fachkräfte);
- Kommunikation und IKT (einschließlich Anbieter von Telekommunikationsdiensten, soziale Netzwerke, andere Plattformen und Internetdienstanbieter);
- Wirtschaft und Finanzen (Banken, Kreditinstitute, Zahlungsdienstleister und Plattformen für elektronische Zahlungsabwicklung).

Die Zusammenarbeit mit diesen Institutionen kann über eine Weiterempfehlung oder Verweisung erfolgen[104].

3.5.3.2. Zentrale Aspekte für eine erfolgreiche Zusammenarbeit

Unabhängig von der benötigten Art der Unterstützung spielt institutionsübergreifende Zusammenarbeit bei der Betreuung von Cyberkriminalitätsopfern allgemein und besonders im Hinblick auf die Erfüllung ihrer sozialen und institutionellen Bedürfnisse aufgrund der Viktimisierungserfahrung (oder Cyber-Viktimisierungserfahrung, in diesem Fall) eine wichtige Rolle.

HIGHLIGHT | WICHTIGSTE INFORMATION:

Das *Policy Paper: challenges in the field of cybercrime and recommendations to overcome them* wurde im Rahmen des ROAR-Projekts der APAV zur Unterstützung von Cyberkriminalitätsopfern erarbeitet und beinhaltet Empfehlungen für die Entwicklung umfassender Cybersicherheitsstrategien. Bereichsübergreifende Zusammenarbeit von politischen Entscheidungsträgern, Exekutivorganen, Justizbehörden, Opferhilfsorganisationen, Industrie, Medien und Kommunikationsunternehmen ermöglicht einen auf das Opfer fokussierten Ansatz und ist ein geeignetes Mittel, um die Bedürfnisse des Opfers angemessen zu erfüllen und den Herausforderungen im Kampf gegen Cyberkriminalität zu begegnen.

Die Zusammenarbeit mit Fachkräften anderer Institutionen und Dienste ist grundlegend für die Qualität der Behandlung des Kriminalitätsopfers.

Die Fachkraft sollte jederzeit in engem Kontakt mit Fachkräften anderer Institutionen oder Dienste stehen, um die richtige Unterstützung und angemessene Reaktion auf die Interessen und Bedürfnisse des Opfers gewährleisten zu können. Die Fachkräfte müssen:

- **vereinfachen**, indem sie die effektive Kommunikation und gute Beziehung zwischen den Fachkräften verschiedener Dienste und Institutionen fördern;
- **fördern**, indem sie die Zusammenarbeit dieser Fachkräfte bei der Minimierung der Auswirkungen von (Cyber-) Kriminalität und angemessenen Betreuung der Opfer unterstützen.

[104] Weitere Informationen zum Thema empfehlen oder verweisen von Opfern siehe Teil II, Kapitel 3, Abschnitt 3.5.1.3 dieses Handbuchs über die Wichtigkeit institutionsübergreifender Zusammenarbeit.

Gemeinsames Handeln kann einige der Hindernisse bei institutionsübergreifender Zusammenarbeit überwinden:

Formalitäten. Die negativen Auswirkungen exzessiver Formvorschriften für den täglichen Kontakt zwischen Institutionen (z. B. langwierige bürokratische Abläufe) sollten reduziert werden, da diese besonders die Geschwindigkeit und Effizienz der Betreuung beeinträchtigen.

Zeit. Die für die Zusammenarbeit verfügbare Zeit (z. B. für die schnelle Weiterleitung eines Berichts) sollte effektiv genutzt werden, ohne die Arbeit anderer Dienste oder Institutionen zu behindern.

Fehlende Praxisorientierung. Beim Kontakt mit anderen Institutionen sollten die Anforderungen des Unterstützungsprozesses möglichst zweckmäßig betrachtet werden.

Fehlende Höflichkeit. Die Fachkraft sollte allen anderen in den Unterstützungsprozess involvierten Fachkräften gegenüber stets höflich sein (z. B. am Telefon, persönlich, per E-Mail etc.).

Kommunikationsfehler. Unklare Kommunikation, die zum Missverständnis von Nachrichten oder Anfragen führen kann, sollte vermieden werden, da diese die Beziehung beeinträchtigen und beträchtlichen Schaden anrichten kann, was sich negativ auf die Qualität der Opferunterstützung auswirkt.

Zurückhaltung von Informationen. Gegenüber Fachkräften anderer Institutionen sollten niemals Informationen zurückgehalten werden, da dies ihre Arbeit am Unterstützungsprozess einschränken oder verzögern kann (z. B. durch einen schlampigen, unvollständigen oder unklaren Bericht, der nicht die erforderlichen Informationen über den Prozessfortschritt enthält).

Reduktive und isolierte Intervention. Die Unterstützung und Weiterempfehlung von Opfern sollte stets umfassend betrachtet werden. Die aktive Teilnahme anderer Fachkräfte von außerhalb des Dienstes oder der Organisation am Netzwerk-Prozess optimiert die verfügbaren Ressourcen.

Wettbewerb. Statt einem Wettbewerb zwischen Diensten oder Institutionen sollte die professionelle Zusammenarbeit gefördert werden, die sich auf die Maximierung der Ressourcen und anderer Angebote der Dienste oder Institutionen konzentriert, um eine möglichst hochwertige und angemessene Intervention zu ermöglichen.

Fehlender persönlicher Kontakt. Fachkräfte anderer Institutionen oder Dienste sollten stets persönlich kontaktiert werden, da so enge Arbeitsbeziehungen geknüpft werden können, über die die erforderlichen Maßnahmen für die Betreuung der Opfer leichter ergriffen werden können.

4. DIE WICHTIGE ROLLE DER PRÄVENTION IM KAMPF GEGEN CYBERKRIMINALITÄT

Verbrechensverhütung ist allgemein als die Gesamtheit aller privaten oder staatlichen Initiativen oder Bemühungen definiert, die Kriminalität zu verhindern versuchen, indem sie entweder das Kriminalitätsrisiko durch eine Veränderung der Risikofaktoren senken und/oder, sollte dies nicht möglich sein, ihre Auswirkungen auf Einzelpersonen und die Gesellschaft abzuschwächen (Copibianco, 2010, Welsh & Farrington, 2012 *cit in* Maia et al., 2016).

Die ersten Versuche zur Verbrechensverhütung wurden im Bereich Konzepte zum Schutz der öffentlichen Gesundheit gemacht. Prävention (von Krankheiten oder Verletzungen) wurde später auch in anderen Bereichen des sozialen Lebens (Bloom, 1996, Doll, Saul, & Elder, 2007 *cit in Saavedra* & Machado, 2010) und sogar gegen Gewalt und Kriminalität und für die Aufrechterhaltung der Sicheheit eingesetzt.

4.1. Ansätze zur Prävention von Cyberkriminalität: zentrale Aspekte

Entsprechend (APAV, 2011) kann Prävention abhängig vom ***Zeitpunkt*** im Verlauf (oder der Entwicklung) eines Verbrechens, an dem sie erfolgt, wie folgt eingeteilt werden:

- **Primäre Prävention**: Intervention vor Auftreten des Problems, um Ausbruch einer Krankheit oder eine Verletzung zu verhindern.

- **Sekundäre Prävention**: Intervention, die auf die Behandlung des Problems abzielt, welches sich im frühestmöglichen Stadium befindet.

  Übertragen auf das Vorkommen von Gewalt und Kriminalität beschreibt sekundäre Prävention Ansätze, die sich auf die unmittelbare Reaktion auf eine Straftat oder Gewalt konzentrieren (z. B. medizinische Versorgung, Notfalldienste).

- **Tertiäre Prävention**: Intervention, die einen Rückfall verhindern, oder die Häufigkeit und Schwere der Schäden vermindern soll.

  Tertiäre Prävention von Gewalt und Kriminalität bezieht sich auf die langfristige Betreuung nach der Tat, wie Rehabilitation, Reintegration und die Reduzierung der Auswirkungen/des Traumas, die aus dem Verbrechen oder der Gewalterfahrung entstanden.

Während sekundäre und tertiäre Prävention von Gewalt und Kriminalität üblicherweise im Umgang mit Opfern Anwendung finden, spielen sie auch im Umgang mit Tätern eine Rolle, besonders durch Justizbehörden.

Prävention kann auch über die ***Interessens***- oder ***Bevölkerungsgruppe*** definiert werden, auf die sie abzielt (APAV, 2011) und wird in diesem Fall wie folgt kategorisiert:

- **Universalprävention**: Ansätze, die sich an Zielgruppen oder die allgemeine Bevölkerung richten, unabhängig vom Risikolevel.

  Beispiele für Ansätze der Universalprävention sind Gewaltpräventionsprogramme für Kinder und Heranwachsende bestimmter Jahrgangsstufen und Aufklärungskampagnen, die sich an die Bevölkerung richten.

- **Selektive Prävention**: Ansätze, die sich an Gruppen oder Personen richten, die im Verhältnis zur allgemeinen Bevölkerung eher gefährdet sind, in Gewalt oder Kriminalität verwickelt zu werden.

  Beispiele hierfür sind Programme zur Förderung der Elternkompetenz Alleinerziehender.

- **Indizierte Prävention**: Interventionsansätze für Hochrisikogruppen, die als Opfer und/oder als Täter bereits Gewalt oder Kriminalität erfahren oder ausgeübt haben.

  Dies schließt zum Beispiel Interventionsprogramme für Beschuldigte der häuslichen Gewalt und Unterstützungsangebote für Kriminalitäts- und Gewaltopfer, die von Opferhilfsorganisationen angeboten werden, ein.

Es gibt weitere Klassifizierungsmöglichkeiten für Präventionsstrategien, zum Beispiel nach dem ***Fokus der Präventionsmaßnahme*** (z. B. UN, 2011 *cit in* Maia et al., 2016; Tonry & Farrington, 1995 cit *in Maia* et al., 2016):

- **Kriminalitätsprävention durch soziale Entwicklung** setzt auf die Verstärkung von Schutzfaktoren und die Reduzierung von Kriminalitätsrisikofaktoren, unter anderem Programme für gefährdete Kinder, die ihnen dabei helfen sollen, sozialen Umgang zu erlernen.

- **Lokale Kriminalitätsprävention** findet in Bezirken mit höherem Kriminalitätsrisiko statt und soll das Sicherheitsgefühl stärken.

- **Verhältnisprävention** soll die Ausübung von Kriminalität so unattraktiv wie möglich machen, indem die Risiken/Kosten, die damit in Verbindung stehen, erhöht und die Gewinnmöglichkeiten reduziert werden.

- **Kriminalitätsprävention über das Justizsystem** erfolgt u.a. durch Reintegration von Straftätern und Präventionsprogramme für Wiederholungstäter.

Abgesehen von der lokalen Kriminalitätspräventionsstrategien können alle o. g. Ansätze auch zur **Prävention von Cyberkriminalität** eingesetzt werden. Prävention von Cyberkriminalität setzt häufig auf Technologie und den Schutz von Computern oder Geräten, während Kriminalitätspräventionsansätze sich eher auf den Faktor Mensch konzentrieren.

4. DIE WICHTIGE ROLLE DER PRÄVENTION IM KAMPF GEGEN CYBERKRIMINALITÄT

Unabhängig der o. g. Präventionsansätze und -typologien hilft das Konzept zum Schutz der öffentlichen Gesundheit[105] Organisationen dabei, Kriminalitäts- und Gewaltpräventions-strategien zu verstehen und umzusetzen. Trotz der Komplexität der Prävention, kann die Planung, Vorbereitung und Umsetzung von Präventionsstrategien in vier Makro-Schritte eingeteilt werden:

1 **Definition des Problems**	• Erfordert, das **Phänomen und seine Dynamik zu verstehen** und sein **Ausmaß und seine Tragweite** in einer bestimmten Gruppe, Gemeinde, Region oder einem Land zu identifizieren (z. B. durch Statistiken über die Anzahl der Meldungen/Anzeigen einer bestimmten Straftat).
2 **Identifikation der Risiko- und Schutzfaktoren**	• **Risikofaktoren**: Charakteristika oder Situationen, die die Wahrscheinlichkeit eines bestimmten Problems erhöhen • **Schutzfaktoren**: Charakteristika oder Situationen, die die Wahrscheinlichkeit eines bestimmten Problems verringern • Präventionsstrategien sollten Risikofaktoren verringern und Schutzfaktoren verstärken
3 **Entwicklung, Test und Bewertung von Präventionsstrategien**	• Präventionsstrategien sollten evidenzbasiert entwickelt werden und sowohl die gestellten Diagnosen als auch die zu lösenden Probleme sowie damit in Verbindung stehende Risiko- und Schutzfaktoren berücksichtigen • **Überwachung** der Präventionsstrategien und **Bewertung ihrer Wirksamkeit** sind erforderlich
4 **Veröffentlichung und Generalisierung**	• Nach der Analyse der Ergebnisse der eingesetzten Präventionsstrategien müssen diese **veröffentlicht** werden, damit sie von anderen Organisationen genutzt werden können

Außerdem, und im Hinblick auf die Prävention von Cyberkriminalität, basiert das von Askerniya (2012) vorgeschlagene Modell für die **Organisation von Präventionsstrategien für Cyberkriminalität** auf vier Säulen, für die Aufklärung das zentrale Element für die Reduzierung von Cyberkriminalität ist (Jahankhani, 2013 *cit in* Al-Ali et al., 2018):

1. **Die Technikkompetenz des einzelnen Nutzers** ist die erste Dimension von Präventionsmaßnahmen gegen Cyberkriminalität. Um das individuelle Risiko zu senken und den persönlichen Schutz zu verbessern, sollten Interventionen darauf abzielen, aufzuklären, Bewusstsein zu schaffen und Nutzern die jeweiligen Fähigkeiten beizubringen, die sie für die sichere Teilnahme an verschiedenen Online-Aktivitäten benötigen (wie das Herunterladen von Musik, Spielen oder Filmen, Onlineshopping und/oder die Nutzung sozialer Netzwerke).

2. Die zweite Dimension umfasst die Reduzierung des Cyberkriminalitätsrisiko durch **Präventionsstrategien, die auf den individuellen Entwicklungsstand des Nutzers angepasst sind**. Hier wird davon ausgegangen, dass das Cyberkriminalitätsrisiko von den Risiko- und Schutzfaktoren abhängt, die mit dem individuellen Entwicklungsstand zusammenhängen, und dass daher das Alter bzw. die Altersgruppe des Nutzers ausschlaggebend für die Entscheidung

[105] Detaillierte Informationen über das Konzept zum Schutz der öffentlichen Gesundheit und Material für die Planung, Umsetzung und Bewertung von Präventionsmaßnahmen sind abrufbar unter https://vetoviolence.cdc.gov/apps/main/home

ist, welche Präventionsstrategien gegen Cyberkriminalität angewendet werden sollen.

3. Die dritte Dimension umfasst das **persönliche Risikoniveau des Nutzers, Cyberkriminalität zu erfahren**, und den Bedarf an Präventionsmaßnahmen, abhängig von Wissensstand, der Ausbildung und des Bewusstseins des Nutzers. Denn:

   - Nutzer mit umfangreichem Wissen über IKT und das Internet, die gut aufgeklärt und sich der Risiken im Cyberspace bewusst sind, haben **ein niedriges Risiko für Cyberkriminalität**.

   - Nutzer mit ungenügendem Wissen und Bewusstsein für die Risiken im Internet weisen ein höheres Risiko für Cyber-Viktimisierung (im Vergleich zur ersten Kategorie) und ein **durchschnittliches Risiko für Cyberkriminalität** auf. Diese Kategorie schließt Personen ein, die sich trotz ihres Wissens über Computer- und Gerätesicherheit der Gefahr nicht ausreichend bewusst sind, um ihr Online-Verhalten und/oder ihre Internet- und IKT-Nutzungsgewohnheiten zu ändern.

   - Nutzer, die das Internet und IKT sehr intensiv nutzen, sich aber über die Gefahren nicht im Klaren sind, haben ein **hohes Risiko für Cyberkriminalität**.

4. Die vierte und letzte Dimension dieses Modells betrifft die **Förderung individueller Fähigkeiten und Verhaltensweisen und die Entwicklung von Interventionsplänen** basierend auf Ausbildung, Aufklärung und Risikobewusstsein im Hinblick auf Online-Risiken und spezifische Verhaltensweisen[106].

Im nächsten Abschnitt stellen wir einige Präventionsmaßnahmen für Cyberkriminalität vor.

4.2. Information, Bewusstseinsschaffung und Aufklärung als Präventionsstrategien

Ausgehend von den Schlüsseldimensionen der o. g. Präventionsstrategien gegen Cyberkriminalität wird klar, wie viel Einfluss Information, Bewusstseinsschaffung und Aufklärung der Internet- und IKT-Nutzer auf deren Verhalten und Fähigkeiten haben, und demzufolge auf die Erhöhung/Reduzierung des Cyberkriminalitätsrisikos.

Die Wahrnehmung der Internet- und IKT-Nutzer ihrer eigenen **Fähigkeiten und Kenntnisse**, sich vor Cyber-Viktimisierung zu schützen, wirkt sich auf ihr Verhalten und ihre Online-Aktivitäten aus. Das gleiche gilt für die Verantwortung für die persönliche Online-Sicherheit (Boehmer et al., 2015; LaRose & Rifon, 2007). Personen, die Cybersicherheit als ihre persönliche Verantwortung sehen und/oder verstehen, dass sie über das Wissen und die Fähigkeiten verfügen, sich vor Cyber-Viktimisierung

[106] Weitere Informationen über Anfälligkeit als Risikofaktor für Cyber-Viktimisierung finden Sie in Teil I, Kapitel 3, Abschnitt 3.2 dieses Handbuchs.

zu schützen, ergreifen (wahrscheinlich) mehr Cybersicherheitsmaßnahmen und verhalten sich umsichtiger, wenn sie das Internet und IKT nutzen.

Dies unterstreicht die Notwendigkeit von **Informations- und Aufklärungskampagnen** sowie **Bildungsprogrammen** (Martin & Rice, 2011; Burns & Roberts, 2013):

- Informations- und Aufklärungskampagnen fördern die sichere und kompetente Nutzung des Internets und IKT;
- Bildungsprogramme vermitteln Wissen, Kenntnisse und Fähigkeiten, die für die Umsetzung von sicheren Online-Verhaltensweisen erforderlich sind.

In jedem Fall müssen Informations-, Aufklärungs- und Bildungsstrategien (Bandura, 1997 *cit in* Lee et al., 2008; Boehmer et al., 2015; Saridakis et al., 2016):

- Explizit über die Risiken informieren, denen Nutzer bei der Verwendung des Internets oder IKT ausgesetzt sein können;
- Riskantes Verhalten identifizieren und Nutzer darauf aufmerksam machen, dass dies ihre Anfälligkeit für Cyber-Viktimisierung erhöhen könnte;
- Das Bewusstsein der Nutzer für bestehende Schutz- und Cybersicherheitsmaßnahmen schärfen, einschließlich objektiver Informationen über die Wirksamkeit verfügbarer Schutzmaßnahmen;
- Die Umsetzung verfügbarer Schutz- und Cybersicherheitsmaßnahmen lehren, z. B. durch direkte Hilfe oder Schritt-für-Schritt-Anleitungen;
- Die positiven Ergebnisse sicheren Online-Verhaltens betonen.

Informations-, Aufklärungs- und Bildungsstrategien können zwar für jeder Altersgruppe durchgeführt werden, aber die Praktiken und Initiativen auf diesem Gebiet konzentrierten sich bisher hauptsächlich auf Kinder und Heranwachsende.

Im Folgenden haben wir eine Übersicht einiger Universalpräventionsmaßnahmen gegen Cyberkriminalität zusammengestellt, einschließlich Initiativen, Programmen und Projekten für Kinder verschiedener Altersgruppen, die auf deren Information, die Förderung von Wissen und die Stärkung der Fähigkeiten für eine sichere Nutzung des Internets und IKT abzielen.

Tabelle II-9: Präventionsprogramme/-projekte gegen Cyberkriminalität – COMMUNICATE SAFELY

Art der Präventionsmaßnahme	Universal
Zielgruppe	Kinder im Alter von 6 bis 18, Eltern und Senioren
Thema/Problem	Sichere Nutzung des Internets
Ziele	• Förderung der IKT-Nutzungskompetenzen; • Freiwilligen-Initiative der Altice-Stiftung mit dem Ziel, das Bewusstsein für die richtige Verwendung von IKT, nämlich Internet und Handys, im Bildungssektor zu schärfen.
Umsetzungsrahmen	Das Programm umfasst Aufklärungsunterricht in Schulen, der nach den Inhalten der Jahrgangsstufen strukturiert ist und alle Schuljahre sowie ein Theaterstück umfasst. Es wird von diversen Online-Ressourcen ergänzt.
Beschreibung	Partnerschaften: • PSP - Polícia de Segurança Pública • Consórcio CIS - Centro Internet Segura, Portugal • ANPRI – Associação Nacional de professores de Informática • RBE – Rede de Bibliotecas Escolares Themen: • Kontrolle durch Eltern • Datenschutz • Passwort • Digitale Identifikationsmöglichkeiten • Veröffentlichung persönlicher Daten und Fotos • Cybermobbing • Gesunde Nutzungsgewohnheiten • Gerätesicherheit (Handys und Computer) • Herunterladen von Anwendungen und Spielen • Betrug/Viren • Online-Käufe • Schadsoftware • Ransomware • Öffentliches W-LAN
Land	Portugal
Weitere Informationen	https://fundacao.telecom.pt/Site/Pagina.aspx?PageId=1975

THINKUKNOW - „JESSIE & FRIENDS"

Art der Präventionsmaßnahme	Universal
Zielgruppe	Kinder im Alter von 4 bis 7 Jahre
Thema/Problem	Internetsicherheit
Ziele	• Wissen, Fähigkeiten und Selbstvertrauen für eine sichere Internet- und IKT-Nutzung fördern • Gelegenheit bieten, wichtige Prinzipien/Werte für die sichere Nutzung des Internets und IKT zu lernen: Respekt für andere; Zustimmung; gesundes und ungesundes Online-Verhalten; Hilfe von vertrauten Erwachsenen zu holen.
Umsetzungsrahmen	In der Gruppe (z. B. in der Schulklasse) und einzeln (Familienkontext)
Beschreibung	• "Jessie & Friends" ist eine Zeichentrickserie mit drei Episoden für Kinder im Alter von 4 bis 7 Jahre: (i) Episode 1 - 4-5 Jahre; (ii) Episode 2 - 5-6 Jahre und (iii) Episode 3 - 6-7 Jahre. • "Jessie & Friends" erzählt die Abenteuer von Jessie, Tia und Mo, wenn die das Internet und IKT nutzen. Die Figuren lernen, dass das Internet nicht nur Spaß macht, sondern auch Risiken birgt. • Es gibt einen Ratgeber zur Serie mit Unterrichtsmaterial für Lehrer, Eltern und/oder Betreuer. • Außerdem gibt es die Geschichten als Buch, um den Lernprozess zuhause oder in der Schule zu vertiefen.
Land	Vereinigtes Königreich
Weitere Informationen	https://www.thinkuknow.co.uk/professionals/resources/jessie-and-friends/

THINKUKNOW - „THINKUKNOW TOOLKIT"

Art der Präventionsmaßnahme	Universal
Zielgruppe	Heranwachsende ab 11 Jahren
Thema/Problem	Internetsicherheit
Ziele	• Eine gesunde Einstellung zu Themen wie Beziehung, Sex oder Internet entwickeln; • Negatives Verhalten in Bezug auf diese Themen identifizieren; • Aufklärung über Anlaufstellen, an denen Rat und Hilfe bezüglich dieser Themen eingeholt werden kann; • Aufklärung über Anlaufstellen, wenn aufgrund von riskanten Online-Situationen Hilfe benötigt wird.
Umsetzungsrahmen	In der Schule
Beschreibung	Aktivitäten: • *Speed finding* – ein Rollenspiel, in dem die Natur von „Online-Freundschaften" unter die Lupe genommen wird und die Risiken und sicheren Möglichkeiten beleuchtet, online Freundschaften zu schließen; • *Digitales Tattoo* – Diskussionen in Paaren oder in der Gruppe; den Jugendlichen wir das Konzept des „digitalen Tattoos" (oder „digitalen Fingerabdrucks") nähergebracht, sowie Wege, damit umzugehen; • *Code Breaker* – Übung, bei der Jugendliche versuchen, die Passwörter fiktiver Figuren zu knacken; • *Thinkuknow Better?* – Jugendliche entwickeln Ratschläge für Gleichaltrige
Land	Vereinigtes Königreich
Weitere Informationen	https://www.thinkuknow.co.uk/professionals/resources/thinkuknow-toolkit/ https://www.src.ac.uk/images/news/658x300/1920/Aug19/StudAct/Thinkuknow_Toolkit.pdf

THINKUKNOW - „JOSH & SUE"

Art der Präventionsmaßnahme	Universal
Zielgruppe	Kinder (keine spezifische Altersgruppe)
Thema/Problem	Internetsicherheit
Ziele	• Jugendliche sollten in der Lage sein, die Konsequenzen unangemessenen Verhaltens im Internet zu verstehen, indem sie an sichere Online-Verhaltensweisen und positives Verhalten in zwischenmenschlichen Online-Beziehungen herangeführt werden
Umsetzungsrahmen	Schule und/oder Familienkontext
Beschreibung	• Den Film gibt es in zwei Versionen, für Jugendliche mit verschiedenen Arten von Lernbehinderungen. • Der Film kann in der Schule und/oder im Familienkontext verwendet werden.
Land	Vereinigtes Königreich
Weitere Informationen	https://www.thinkuknow.co.uk/parents/Support-tools/Films-to-watch-with-your-children/Josh_and_Sue_original1/

ZUKY'S SAFETY GUIDE

Art der Präventionsmaßnahme	Universal
Zielgruppe	Kinder (keine spezifische Altersgruppe)
Thema/Problem	Internetsicherheit
Ziele	• Kinder über die Risiken im Internet, Cybersicherheitsmaßnahmen und persönliche Schutzmaßnahmen informieren
Umsetzungsrahmen	Kann in jedem Kontext eingesetzt werden, durch Familie, Betreuer und/oder Fachkräfte
Beschreibung	• Zeichentrickserie für Kinder mit der Hauptfigur „Zuky", einem Superhelden für Internetsicherheit. Die Serie kann auf der Homepage oder auf Youtube angesehen werden. Auf der offiziellen Homepage gibt es neben den Videos auch Ratgeber und Quiz für Kinder, ebenso wie Informationsmaterial über Internetsicherheit für Familien und Erziehungsberechtigte.
Land	Niederlande
Weitere Informationen	https://www.paloaltonetworks.com/campaigns/kids-in-cybersecurity https://www.youtube.com/channel/UCDYFyxEbTw0oF0FdzP1hlfg https://trailhead.gsnorcal.org/wp-content/uploads/2018/12/EN_PANE_0nepaper_Kids_in_Cybersecurity.pdf

PROJECT deSHAME

Art der Präventionsmaßnahme	Universal
Zielgruppe	Jugendliche im Alter von 13 bis 17 Jahren
Thema/Problem	Sexuelle Belästigung im Internet
Ziele	• Jugendliche dazu ermutigen, sexuelle Belästigung im Internet[107] zu melden • Verbesserung bereichsübergreifender Zusammenarbeit bei der Prävention und im Umgang mit solchem Verhalten
Umsetzungsrahmen	Gemeinde und Schule
Beschreibung	Das deSHAME-Projekt wird von der Europäischen Kommission gefördert und soll sexuelle Belästigung im Internet bekämpfen. Es handelt sich um eine Kooperation zwischen *Childnet* (Vereinigtes Königreich), *Save the Children* (Dänemark), *Kek Vonal* (Ungarn) und *UCLan* (Vereinigtes Königreich). Das Projekt umfasst die Entwicklung pädagogischer Ressourcen, um sexuelle Belästigung im Internet zu verhindern und dessen Meldung zu ermöglichen. In diesem Rahmen wurde das *Step Up, Speak Up!*-Toolkit entwickelt – ein Leitfaden für aktiven Unterricht für Jugendliche, in dessen Rahmen sexuelle Belästigung im Internet angesprochen wird. Ressourcen und Infomaterialien für die Schule wurden ebenfalls entwickelt.
Land	Verschiedene
Weitere Informationen	https://www.childnet.com/our-projects/project-deshame https://www.childnet.com/ufiles/Project_deSHAME_Dec_2017_Report.pdf

[107] Das Projekt definiert sexuelle Belästigung im Internet als seine Reihe ungewollter, sexueller Verhaltensweisen, die auf jeder digitalen Plattform erfolgen können. Dieses umfangreiche Konzept bezieht verschiedene Formen der Cyberkriminalität/Gewalt mit ein, die in Teil I, Kapitel 1 dieses Handbuchs behandelt werden, einschließlich Cybermobbing, unerlaubte Veröffentlichung von Bildern und Videos und verschiedene Formen des sexuellen Missbrauchs und der sexuellen Ausbeutung von Kindern über das Internet.

KIDS IN THE KNOW – „ZOE & MOLLY ONLINE"

Art der Präventionsmaßnahme	Universal
Zielgruppe	Grundschule, erste Jahre weiterführender Schule
Thema/Problem	Internetsicherheit
Ziele	• Schüler müssen Risiken und Vorteile bei der Internetnutzung erkennen können • Schüler sollten wissen, wie sie sicher auf Risiken reagieren können, denen sie online begegnen
Umsetzungsrahmen	In der Schule Es gibt ebenfalls eine Webseite mit Spielen, Quiz und Comics, die in der Schule oder zusätzlich zuhause verwendet werden können.
Beschreibung	• *"Zoe & Molly Online"* ist ein Comic-Heft. *„Zoe & Molly Online"* wurde vom Kanadischen Kinderschutzzentrum entwickelt, um im Unterricht die Sprache auf die Risiken im Zusammenhang mit dem Veröffentlichen persönlicher Informationen im Internet zu bringen. • Außerdem sollen Eltern in den Prozess miteinbezogen und ihnen die Aufsicht erleichtert werden, indem die Kinder ermutigt werden, erst mit einem vertrauenswürdigen Erwachsenen zu sprechen, bevor sie im Internet jemandem Informationen geben.
Land	Kanada
Weitere Informationen	http://www.zoeandmolly.ca/pdfs/zm_TeacherKit_SinglePagesGr4_en.pdf https://www.zoeandmolly.ca/app/en/

4.2.1. Das Beispiel öffentlicher Informations- und Aufklärungskampagnen

Die Medien sind ein mächtiges Werkzeug für die Verbreitung von Inhalten und spielen bei der Prävention von Gewalt und Kriminalität auf mehreren Ebenen eine zentrale Rolle (APAV, 2011).

Sie können ein wichtiger Kanal für Cyberkriminalitätsprävention sein, besonders durch die Verbreitung öffentlicher Informations- und Aufklärungskampagnen in diesem Feld, entweder über verschiedene Medien, einschließlich dem Internet und sozialen Netzwerken, oder über traditionellere Medien wie das Fernsehen. In jedem Fall sollten Informations- und Aufklärungskampagnen als breiter Ansatz für Cyberkriminalitätsprävention eingesetzt werden (Brewer et al., 2019).

Die Kampagnen haben verschiedene Ziele, (Finn & Banach, 2000; Brewer et al., 2019), wie:

- Das Bereitstellen von Informationen über Cybersicherheitsmaßnahmen und persönliche Schutzmaßnahmen für die Nutzung des Internets und IKT;

HIGHLIGHT | ANGEBOTE IM FOKUS:

Die *Agentur der Europäischen Union für Cybersicherheit* (ENISA) betreibt die jährliche Aufklärungskampagne *European Cyber Security Month*.

Diese europäische Kampagne soll das Bewusstsein für Cybersicherheitsbedrohungen schärfen und Einzelpersonen und Organisationen das Thema Cybersicherheit näherbringen.

Sie stellt auch Ressourcen für den persönlichen Schutz, Informationen über eine Reihe von Aufklärungsinitiativen und Austausch bewährter Methoden bereit.

Frühere Kampagnen und deren Material, einschließlich Videos und Infografiken, sind abrufbar unter https://cybersecuritymonth.eu/press-campaign-toolbox/infographics

Alle Informationen über die Initiative *European Cyber Security Month* sind abrufbar unter https://cybersecuritymonth.eu/

- Förderung positiver Verhaltensweisen und Werte in Verbindung mit Internet- und IKT-Nutzung;

HIGHLIGHT | ANGEBOTE IM FOKUS:

Die *European Cyber Security Month*-Kampagne 2019 informierte unter dem Motto Cyber-Hygiene über die Wichtigkeit gesunder und sicherer Nutzung des Internet und IKT im Alltag.

Sämtliches Material der Kampagne ist abrufbar unter: https://cybersecuritymonth.eu/#/campaign

Die *European Cyber Security Month*-Kampagne und die Agentur der *Europäischen Union für Cybersicherheit* stellen eine breite Auswahl an Informations- und Aufklärungsmaterial zur Verfügung.

Unter ihnen tut sich besonders das *Netzwerk- und Informationssicherheits-Quiz (NIS)*hervor: Ein Selbstdiagnosesystem, mit dem das Niveau der Kenntnisse und Fähigkeiten von Themen wie Cybersicherheit im Allgemeinen, Datenschutz und Cybersicherheitsbedrohungen ermittelt werden kann.

Dieses Tool ist in verschiedenen Sprachen verfügbar und ist erreichbar unter: https://cybersecuritymonth.eu/references/quiz-demonstration/welcome-to-the-network-and-information-security-quiz/

- Über angemessenes Verhalten in Cyber-Viktimisierungssituationen zu informieren;

HIGHLIGHT | ANGEBOTE IM FOKUS:

Die Aufklärungskampagne *Say No!* von EUROPOL soll Kindern und Jugendlichen bewusst machen, wie sie sexuelle Erpressung von Kindern im Internet erkennen und behandeln müssen, und betonen, wie wichtig es ist, solche Vorfälle zu melden und sich Unterstützung zu suchen.

Die Kampagnenvideos (in verschiedenen Sprachen) und weiteres Informationsmaterial sind abrufbar unter: https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/online-sexual-coercion-and-extortion-crime

- Gegenseitige Unterstützung oder Einbeziehung Dritter in die Etablierung von Schutz- und Sicherheitsmaßnahmen im Internet zu fördern (z. B. die Rolle der Familie bei der Identifizierung der Risiken im Hinblick auf das Surf-Verhalten des Kindes);

- Cyberkriminalität zu verhindern, indem über die damit zusammenhängenden Risiken und negativen Konsequenzen aufgeklärt wird.

HIGHLIGHT | ANGEBOTE IM FOKUS:

EUROPOL startete mit für eine andere Zielgruppe die Aufklärungskampagne *Cyber crime vs. cyber security: what will you choose?* (Dt. etwa: Cyberkriminalität vs. Cybersicherheit: Wofür entscheiden Sie sich?)

Die Kampagne ist in verschiedenen Sprachen verfügbar und richtet sich an Jugendliche, die über die Konsequenzen und Kosten einer Verwicklung in illegale Aktivitäten wie Cyberkriminalität informiert und so davon abgehalten werden sollen.

Das Material der Kampagne kann heruntergeladen werden unter: https://www.europol.europa.eu/publications-documents/cyber-crime-vs-cyber-security-what-will-you-choose-poster

Im Rahmen dieser Initiative stellt EUROPOL auch Informationen und Ratgeber für Jugendliche, Familien und Betreuungskräfte zur Verfügung.

4.3. Die Rolle der Familie bei der Prävention

Die Erwachsenen der momentanen Generation sind, anders als Kinder und Jugendliche, nicht als „Digital Natives" aufgewachsen und akzeptieren das Internet und IKT nicht so schnell als natürlichen, fundamentalen und nicht zu hinterfragenden Bestandteil ihres Lebens. Ihre effiziente Nutzung des Internets und IKT wird nicht nur häufig durch ihr begrenztes Wissen und mangelnde Fähigkeiten beschränkt, die Familie ist sich der Online-Aktivitäten von Kindern und Jugendlichen oft nicht wirklich

bewusst (Richardson & Milovidov, 2019; Cross et al., 2016; Lwin et al., 2013; Öztürk & Akcan, 2016).

Paradoxerweise spielen die Erwachsenen in der Familie eine ausschlaggebende Rolle bei der Informierung und Aufklärung von Kindern und Jugendlichen über die sichere Nutzung des Internets und IKT und entsprechend auch bei der über die Prävention von Cyber-Viktimisierung und riskanten Online-Verhaltensweisen (Mesch, 2009; Notar et al., 2013; Morais, 2012 *cit in* Martins et al., 2017; Smallbone & Wortley, 2017; Richardson & Milovidov, 2019).

Dementsprechend spielt die Familie bei einer Reihe von Faktoren eine wichtige Rolle:

- Bei der Aufstellung und Umsetzung **konsistenter Regeln** für den Umfang mit dem Internet und IKT durch Kinder und Jugendliche unter der Verantwortlichkeit der Erwachsenen;
- Bei der Aufklärung von Kindern und Jugendlichen über ihre **Rechte und Pflichten** bei der Nutzung des Internets und IKT;
- Bei der **Förderung von Empathie** und Respekt für andere in jedem Kontext, auch online;
- Bei der **Information** und Unterstützung von Kindern hinsichtlich Fragen der Privatsphäre, Cybersicherheit und persönlicher Schutzmaßnahmen bei der Nutzung des Internets und IKT sowie bei der **Aufklärung über Risiken**, die dabei auftreten können, einschließlich Gewalt und Kriminalität;
- Bei der **Überwachung der Internet- und IKT-Nutzung** durch offene Kommunikation. Die Erziehungsberechtigten erlernen die richtige Internet- und IKT-Nutzung, vermitteln dieses Wissen und zeigen Interesse an den Online-Aktivitäten der Kinder und Jugendlichen;
- Bei der Identifizierung möglicher **Anzeichen für Cyber-Viktimisierung** (oder ungesunder Internet- und IKT-Nutzungsgewohnheiten) bei Kindern und Jugendlichen und entsprechender Einleitung angemessener Interventions-/Schutzmaßnahmen im Fall eines Cyber-Verbrechens;
- Aufrechterhaltung der **Kommunikationskanäle** von Kindern und Jugendlichen, damit diese sich bei Cyber-Viktimisierung oder anderen Fällen, in denen ihr persönlicher Schutz im Internet oder über IKT angegriffen wird, Unterstützung/Hilfe von Erwachsenen holen können, denen sie vertrauen.

HIGHLIGHT | ANGEBOTE IM FOKUS:

INTERNETMATTERS.ORG ist eine Non-Profit-Organisation, die Familien dabei unterstützt, Kindern und Jugendlichen eine sichere Nutzung des Internets und IKT zu ermöglichen.

Die Plattform stellt Informationen, Ratgeber und spezifische Materialien für Familien mit Kindern und Jugendliche verschiedener Altersgruppen zur Verfügung.

Sie informiert außerdem über die verschiedenen Arten von Cyberkriminalität, die Kinder und Jugendliche betreffen können, wie u. a. Cyber-Grooming, Cybermobbing, Identitätsdiebstahl im Internet.

Zugang zur Plattform erhalten Sie unter: https://www.internetmatters.org/

PARENTINFO.ORG ist auch eine Plattform für Eltern und Familien, mit Informationen und Empfehlungen über

eine breite Auswahl an Themen des Internets und IKT, u. a. Cybersicherheit, Anwendungen und Technologie, Wohlbefinden und Gesundheit.

Zugang zur Plattform erhalten Sie unter: https://parentinfo.org/

Im Hinblick auf die Rolle der Familie in der Cyberkriminalitätsprävention wurde das Konzept des *Digital Parenting* entwickelt, das auf den folgenden Prinzipien beruht:

- Offene Kommunikation zwischen Familie/Eltern und deren kleinen oder jugendlichen Kindern;
- Einbeziehung der Familie/Eltern in die Online-Aktivitäten der Kinder und Jugendlichen auf die gleiche Weise, wie es bei den *herkömmlichen* Alltagsaktivitäten der Fall ist;
- Schutz der digitalen Identität der Kinder und Jugendlichen, d. h. der Art und Weise, wie sich das Kinder oder der oder die Jugendliche online präsentiert oder darstellt;
- Gemeinsames Lernen der Familie/Eltern und deren kleinen oder jugendlichen Kindern;
- Schutz der abhängigen Kinder und Jugendlichen vor den Risiken und Bedrohungen des Internets und der IKT, insbesondere vor Cyberkriminalität.

HIGHLIGHT | ANGEBOTE IM FOKUS:

Der Europarat ließ den Ratgeber *Kindererziehung im digitalen Zeitalter; Empfehlungen für Eltern, wie sie Kinder vor sexueller Ausbeutung und sexuellem Missbrauch im Internet schützen können* veröffentlichen.

Darin finden Eltern und Familien Informationen über die verschiedenen Formen sexuellen Missbrauchs und Ausbeutung von Kindern im Internet. Der Ratgeber enthält praktische und informative Tipps und Materialien, die Eltern und Familien dabei helfen sollen, Kinder und Jugendliche vor diesen Phänomenen zu schützen oder sich richtig zu verhalten, wenn bereits eine Cyber-Viktimisierung eingetreten ist.

Der Ratgeber ist abrufbar unter https://rm.coe.int/digital-parenting-/16807670e8

Der Europarat stellt außerdem eine Reihe anderer Informations- und Aufklärungsmaterialien über den Schutz von Kindern und Jugendlichen im Internet zur Verfügung. Das *Internet Literacy Handbook*, des Europarats kann zum Beispiel hier heruntergeladen werden: https://www.coe.int/en/web/children/internet-literacy-handbook.

Siehe auch https://www.coe.int/en/web/children/the-digital-environment für weitere Informationen.

4.4. Die Schule als wichtiger Präventionskontext

Neben der Familie ist die Schule ein **sehr wichtiger Sozialisierungskontext** für die Entwicklung von Kindern und Jugendlichen, nicht nur für den Bildungserwerb, sondern auch für das Erlernen **sozialer Verhaltensweisen für das spätere Leben**. Dabei handelt es sich um grundlegende Fähigkeiten, die Kinder oder Jugendliche

brauchen, um ihren Platz in der Gesellschaft einnehmen zu können oder um mit der Welt um sie herum in Beziehung treten zu können (Saavedra & Machado, 2010), ganz besonders in engen Beziehungskontexten mit Gleichaltrigen oder der Familie. Die Qualität des Verhältnisses zwischen Kindern und Jugendlichen und der Schule ist ein weitere Schutzfaktor gegen riskantes Verhalten. Daher müssen Schulen Gelegenheiten fördern, die das Wohlbefinden und positive Beziehungen der Kinder und Jugendlichen zu ihren Klassenkameraden und dem Lehrpersonal verbessern (McNeely, Nonnemaker, & Blum, 2002 cit *in Saavedra* & Machado 2010).

Die Schule ist ein natürlicher Kontext für die Umsetzung von Kriminalitäts- und Gewaltpräventionsinitiativen, da die meisten Kinder zur Schule gehen und in diesem Umfeld einen großen Teil ihrer Zeit verbringen (Durlak, 1995 *cit in idem*).

Die folgende Tabelle enthält eine Übersicht der Merkmale, die für die Effektivität von Präventionsprogrammen im schulischen Umfeld erforderlich sind (APAV, 2011; Brewer et al., 2019)

Tabelle 8: Hauptbestandteile schulischer Präventionsprogramme

Schlüssige theoretische Grundlage: Der Ausgangspunkt für die Planung muss eine klare, theoretische Grund-lage mit evidenzbasierten Erkenntnissen aus der Forschung sein.

Umfassender Ansatz: Das Programm sollte sich nicht allein auf das Individuum konzentrieren, sondern auch auf sein oder ihr soziales Umfeld: Familie, Schule, Gemeinde. Schulische Interventionsprogramme sind am erfolgreichsten, wenn sie von der Familie oder dem sozialen Umfeld ergänzt werden, da diese Verhaltensän-derungen verstärken und fördern können.

Ganzheitliches Herangehen an Risiko- und Schutzfaktoren: Programme müssen so entwickelt werden, dass sie Risikofaktoren vermindern und gleichzeitig Schutzfaktoren stärken.

Individuelle Anpassung: Das Programm sollte entsprechend der Bedürfnisse des Individuums/der Gruppe entwickelt werden; es sollte zum Alter, Entwicklungsstand und den Merkmalen der Zielgruppe passen.

Frühe und an die Entwicklung angepasste Intervention: Die Intervention sollte so früh wie möglich erfolgen, entsprechend dem Entwicklungsstand des Individuums.

Auswahl des richtigen Ziels: Wissensmehrung, Veränderung von Verhaltensweisen und Einstellungen und das Erlernen neuer Fähigkeiten sind die vielversprechendsten Angriffspunkte, um Veränderungen zu bewirken.

Einbeziehung Gleichaltriger: Da Gleichaltrige enormen Einfluss auf Individuen ausüben, gibt es Präventionsprogramme, die auf den Rückhalt in der „Peer Group" als Präventionsmaßnahme setzen.

Interaktive Informationsvermittlungsmethoden: Aktivitäten sollten so interaktiv, ansprechend und altersgemäß wie möglich durchgeführt werden: Diskussionsgruppen, Debatten, Brainstorming, Rollenspiele etc.

Systematisches Lernen und Festigen: es müssen Gelegenheiten für das Training sozialer Fertigkeiten geschaffen werden: Konfliktlösung, Durchsetzungsfähigkeit, Entscheidungsfindung, aktives Zuhören; ebenso wie Festigung durch kognitives Verhaltenstraining wie Rollenspiele, Simulationen realitätsnaher Situationen und der Erfahrungen der Teilnehmer etc.

Förderung des sozialen Bewusstseins: Präventionsprogramme können den Teilnehmern helfen, die Gefühle und Gedanken anderer zu verstehen (Empathie) und positive Interaktion mit verschiedenen Gruppen zu schätzen zu wissen.

Emotionsmanagement: Präventionsprogramme helfen den Teilnehmern effizient und angemessen mit ihren Emotionen umzugehen (Management der eigenen Emotionen).

Fokus auf Beziehungen: Präventionsprogramme bereiten Teilnehmer darauf vor, positive Beziehungen zu anderen aufzubauen, fördern ihre Fähigkeit zu kommunizieren, kooperieren, verhandeln, Konflikte zu lösen, Hilfe zu suchen (sofern erforderlich) und auf angemessene Weise auf Druck unter Gleichaltrigen oder Herausforderungen des sozialen Umfelds zu reagieren.

Ausbildung, Betreuung und interdisziplinäre Zusammenarbeit: Die Vorbereitung der Fachkraft ist ausschlag-gebend für die Qualität und den Erfolg des Programms.

Genderneutraler Ansatz: Die Geschlechteridentität der Rezipienten muss respektiert und im Interventionsprozess berücksichtigt werden.

Fokus auf der normativen Ebene des Problems: Neben den schweren Formen der Gewalt sollten Präventionsprogramme auch die normativen Ebenen der Gewalt (einschließlich subtiler Formen, die gewöhnlich von der Zielgruppe toleriert oder sogar als normal angesehen werden) berücksichtigen.

Alternative Verhaltensweisen: Im Rahmen der Intervention müssen alternative Verhaltensweisen aufgezeigt werden, die nicht auf unangemessenem Verhalten beruhen.

Information: Programme müssen über Risikofaktoren, die Konsequenzen bestimmter Verhaltensweisen und soziale Unterstützungsstrukturen aufklären.

Eindeutige Botschaft und leicht verständliche Materialien: Die Programme sollten über nutzerfreundliche Anleitungen und/oder Beschreibungen verfügen, um die Umsetzung zu erleichtern.

Vollständige Umsetzung des Programms: Die Programme müssen vollständig umgesetzt werden und die gesetzten Ziele erfüllen. Dazu benötigen sie Abläufe, mit denen die Umsetzung überwacht werden kann.

Intensive und langfristige Intervention: Präventionsprogramme sind intensiv und langfristig angelegt.

Evaluation: Präventionsprogramme benötigen eine unabhängige (nicht dem Konzeptions- oder Umsetungsteam zugehörige) Beurteilung der Veränderung in den Zielgruppen, die durch die Anwendung verifizierter Methodik erreicht werden konnten.

Nachhaltigkeit: Die Vorteile der Umsetzung und ihre langfristige Nachhaltigkeit müssen gegen die Kosten abgewogen werden.

HIGHLIGHT | ANGEBOTE IM FOKUS:

NoTrap! ist ein italienisches Online-Interventionsprogramm für Schulen, das Mobbing und Cybermobbing verhindern soll.

IKT sind der Ausgangspunkt des Programms, das auf zwei grundlegenden Annahmen basiert:

- Die Nutzung von IKT kann das Risiko für Cybermobbing erhöhen.
- IKT können auch als Werkzeug genutzt werden, um das Wissen und die Fähigkeiten zur Prävention und Verhinderung von Cybermobbing zu trainieren und zu stärken.

Evaluierungsstudien über das Programm beweisen, dass Mobbing und Cybermobbing reduziert werden konnten (Palladino et al., 2016).

HIGHLIGHT | ANGEBOTE IM FOKUS:

Beim Projekt *CyberTraining: A Research-based Training Manual On Cyberbullying* untersuchen Forscherteams aus Deutschland (verantwortlich für die Koordination), Portugal, Spanien, dem Vereinigten Königreich, Irland und Experten für Informations- und Kommunikationstechnologien und digitale Kultur aus Bulgarien, der Schweiz und Norwegen das Phänomen des Cybermobbings.

Im Rahmen des Projekts wurde ein Leitfaden über den Umgang mit Cybermobbing erstellt, der sich in erster Linie an Fachkräfte richtet, die mit dem Thema arbeiten, aber verschiedene Zielgruppen bedienen, besonders Jugendliche, Familien und Schulen. Zusätzlich zum Theorieteil enthält der Leitfaden auch Anleitung, Unterstützung und Material für die Prävention und Bekämpfung des Problems (Matos et al., 2011).

4.5. Prävention für anfällige Gruppen: Kinder und Jugendliche

Als sogenannte Digital Natives zeigen Kinder und Jugendliche ein **beinahe natürliches Interesse an Online-Aktivitäten**. Während dies viele Vorteile hat, erhöht es andererseits **die Anfälligkeit dieser Gruppe, in cyberkriminelle Aktivitäten verwickelt zu werden**, sowohl als Opfer als auch als Täter (Alkan & Citak, 2007 cit *in Edirisuriya* & Liyanage, 2016).

Für diese Gruppe ist die Kommunikation über internetgestützte Kommunikationsmittel und virtuelle Netzwerke keine technologische Subkultur, sondern ein Weg, um den Kontakt mit Gleichaltrigen aufrechtzuerhalten. Die Kommunikation über solche Medien scheint von dieser Altersgruppe bevorzugt zu werden, da sie mehr Privatsphäre und Anonymität bietet und auf Kosten der Kommunikation von Angesicht zu Angesicht Enthemmung begünstigt (Chisholm, 2014).

Jugendliche bewegen sich ganz natürlich durch das Internet und IKT und sind daher nicht selten an illegalen Online-Aktivitäten beteiligt, entweder aus Sensationslust, zum Spaß oder weil sie mit ihrem Verhalten keine negativen Konsequenzen in Verbindung bringen. Das oben zusammengefasste ANGEBOT IM FOKUS – die Aufklärungskampagne *Cyber crime vs cyber security: what will you choose?* von EUROPOL – informiert über und warnt vor den Konsequenzen der Beteiligung an illegalen Online-Aktivitäten und versucht, positive und normative Verhaltensweisen zu fördern.

Das Risiko für Cyber-Viktimisierung ist unter Jüngeren entsprechend höher. Die *STATISTIKEN IM FOKUS* in Teil I, Kapitel 1 dieses Handbuchs legen die dieser Aussage zugrundeliegenden Daten dar.

HIGHLIGHT | ANGEBOTE IM FOKUS:

Ergänzend zu der o. g. Aufklärungskampagne von EUROPOL über sexuelle Erpressung im Internet bietet die Kampagne *YOUR LIFE IS ONLINE. PROTECT IT!* viele Informationen für Jugendliche, die ihnen bei der Reduzierung des Risikos und der Anfälligkeit helfen sollen, die aus ihrem Online-Verhalten entstehen.

Sie umfasst Informationen über Cybersicherheitsmaßnahmen, deren Umsetzung die **digitale Privatsphäre** besonders in sozialen Netzwerken verbessert und über **persönliche Schutzmaßnahmen**, die das Cyber-Viktimisierungsrisiko senken.

Siehe https://www.europol.europa.eu/how-to-set-your-privacy-settings-social-media

Abgesehen davon stellt *YOUR LIFE IS ONLINE. PROTECT IT!* auch Informationen und Anweisungen zur Verfügung, wie man sich in Situationen von Cyber-Viktimisierung verhält, wie zum Beispiel:

- Wie fordert man die Entfernung von Inhalten auf verschiedenen Plattformen an, wenn Bilder und Videos unerlaubt veröffentlicht wurden: https://www.europol.europa.eu/removing-links-to-explicit-content
- Wie meldet man Fälle von Cyber-Viktimisierung und wo erhält man Hilfe: https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/are-you-victim-get-help-report-it-we-are-here

4.6. Situative Cyberkriminalitätsprävention: eine Frage der Gelegenheit

Situative Kriminalitätsprävention ist ein theoretisches Paradigma, das sich auf Gelegenheiten für kriminelle Handlungen konzentriert und wie die Umgebung, Bedingungen und der Kontext verändert werden können, um diese Gelegenheiten zu verhindern. Dieses Paradigma beruht auf der Theorie der rationalen Entscheidung und der[108] Routine-Activity-Theorie (Hinduja & Kooi, 2013):

- Die Theorie der rationalen Entscheidung setzt auf der Mikro-Ebene an und geht davon aus, dass kriminelle Verhalten von einer Zielsetzung angetrieben wird, die zu einem Vorteil führt. Entsprechend könnten Veränderungen in der Struktur der Gelegenheit die Wahrnehmung von Risiko, Aufwand und Belohnung verändern.
- Die Routine-Activity-Theorie geht von der Makro-Ebene aus und zeigt, dass Veränderungen des Alltags die Bewegungen wahrscheinlicher Kriminalitätsziele, die letztendliche Handlungswahrscheinlichkeit durch den Täter und das Niveau der Überwachung beeinflussen.

Situative Kriminalitätsprävention widmet sich dem Veränderungspotenzial der Umgebung, in der Kriminalität vorkommt, das diese Umgebung weniger attraktiv für motivierte Täter macht. Kriminalitätsprävention hängt entsprechend davon ab, die Gelegenheiten des Täters von Anfälligkeiten zu profitieren zu reduzieren, indem die Umgebung verwaltet, gestaltet und verändert wird, d. h. indem **in der Umgebung Hürden geschaffen werden, die die Wahrscheinlichkeit**

[108] Kriminologische Theorien (und ihre Anwendung zum Verständnis von Cyberkriminalität) werden in Teil I, Kapitel 3, Abschnitt 3.1 dieses Handbuchs behandelt.

krimineller Gelegenheiten mindern. Im Idealfalls tragen diese Bemühungen dazu bei Risiko und Aufwand für eine illegale Aktivität zu erhöhen und **die Belohnung für eine erfolgreich verübte Straftat zu verringern**. Können Existenz und Attraktivität krimineller Gelegenheiten reduziert werden, wird das Ergebnis eine Reduzierung der Kriminalität sein (Clarke, 1997cit *in* Hinduja & Kooi, 2013).

Über die Jahre wurde eine Reihe von Vorschlägen und spezifischen Interventionsmaßnahmen für Umgebungen erarbeitet, in denen Kriminalität vorkommt – sie werden als **situative Präventionstechniken bezeichnet**. Deren Hauptziel ist die Reduzierung der Gelegenheiten für das Vorkommen von Kriminalität durch die Veränderung der Umweltbedingungen. Es gibt fünf Kategorien der situativen Prävention, von denen jede Kategorie fünf spezifische Anwendungstechniken beinhaltet (Cornish & Clarke, 2003 cit *in* Agustina, 2015):

Kategorie *Aufwand erhöhen*:

Wenn der Aufwand für eine bestimmte Straftat erhöht wird, hält das den Täter unter Umständen davon ab, diese zu begehen.

Diese Kategorie beinhaltet 5 Techniken:

- Ziel sichern (Einrichtung von Barrieren, um den Zugang zum Opfer zu erschweren);
- Zugang zu Einrichtungen kontrollieren (Zugang zu *Orten*, an denen kriminelle Handlungen auftreten können);
- Ausgänge kontrollieren (Ausgang/Bewegungen an einem *Ort* kontrollieren);
- Täter umlenken (Bewegungsmuster potenzieller Täter verändern)
- Waffen/Werkzeuge kontrollieren (Zugang zu Mitteln beschränken, die zum *Modus Operandi* gehören).

Kategorie *Risiken erhöhen*:

Diese Techniken sollen das Risiko des Täters, gefasst zu werden, erhöhen:

- Schutzmaßnahmen verstärken/Bewachung ausweiten (Schaffung von Maßnahmen, durch die sich Menschen sicherer fühlen; zum Beispiel Nachbarschaftswachen);
- Natürliche Überwachung stärken (z. B. Verbesserung der Beleuchtung eines Ortes);
- Anonymität reduzieren;
- Informelle Überwachung (z. B. durch verstärkte Bewegung der Mitarbeiter in einem Geschäft);
- Formelle Überwachung (z. B. durch verstärkte Polizeipräsenz).

Kategorie *Belohnung verringern*:

Diese Kategorie zielt darauf ab, die Belohnung zu verringern, die ein potenzieller Täter für die Ausübung einer Straftat erhält.

Die wichtigsten Techniken sind:

- Ziele verbergen (z. B. in privater Garage parken, statt auf der Straße oder an öffentlichen Orten);
- Ziele entfernen (z. B. Elektrogeräte und andere Waren mitnehmen, wenn das Auto geparkt wird);
- Besitz kennzeichnen (z. B. Fahrzeug registrieren);
- Märkte stören (z. B. Lizenzpflicht für Dienstleistungen oder Handel);
- Belohnung verwehren (z. B. durch die Nutzung eines Handypassworts).

Kategorie *Provokation reduzieren*:

Diese Kategorie reduziert Auslöser für kriminelles Verhalten.

Die wichtigsten Techniken sind:

- Frustration und Stress reduzieren (z. B. über Ankunft/Wartezeit öffentlicher Verkehrsmittel informieren);
- Streit vermeiden (z. B. Fans bei Fußball-/Sportveranstaltungen trennen);
- Emotionale Erregung reduzieren (z. B. Gewaltdarstellung in Medien kontrollieren);
- Druck durch Gleichaltrige neutralisieren (z. B. durch Aufklärungskampagnen);
- Nachahmung verhindern (z. B. Orte sauber halten und Spuren von Vandalismus schnell entfernen).

Kategorie *Ausflüchte verhindern*:

Die Kategorie enthält die folgenden situativen Präventionstechniken:

- Regeln aufstellen;
- Anweisungen klar zeigen (z. B. durch „Parken verboten" Schilder);
- Bewusstsein schaffen (z. B. durch Aufklärungskampagnen, die darüber informieren, dass dieses Verhalten illegal ist);
- Einhaltung erleichtern (z. B. bei Veranstaltungen den Zugang zu öffentlichen Verkehrsmitteln erleichtern);
- Alkohol- und Drogenkonsum kontrollieren (z. B. pro Person Obergrenze für alkoholische Getränke in Clubs).

Situative Präventionsansätze werden in herkömmlichen Kontexten häufig eingesetzt und haben sich bei der Reduzierung verschiedener Arten herkömmlicher Straftaten als wirksam erwiesen. Die Relevanz situativer Prävention von Cyberkriminalität wurde ebenfalls analysiert (Brewer et al., 2019).

In diesem Zusammenhang erarbeitete Miró Llinares (2012, *cit in* Agustina, 2015) eine Kombination aus **konkreten situativen Präventionsmaßnahmen gegen Cyberkriminalität**:

Tabelle 9: Situative Präventionstechniken gegen Cyberkriminalität

Reduzierung der Häufigkeit von Gelegenheiten	Wahrgenommenen Aufwand erhöhen	Wahrgenommenes Risiko erhöhen	Erwartete Belohnung verringern	Ausflüchte eliminieren
Ziele nicht vorstellen	Kontrolle des Systemzugangs	Bewachung/ Überwachung ausweiten	Ziele verbergen	Regeln aufstellen
Risikozonen identifizieren	Angriff feststellen und verhindern	Anonymität reduzieren	Ziele entfernen	Regeln aufstellen
Dekontaminierung/ Beseitigung von Rückständen	Täter umlenken	Formelle Überwachung verstärken	Vorteile entfernen	Moralisches Bewusstsein stärken
Ziele trennen	Waffen/Werkzeuge kontrollieren	Natürliche Überwachung unterstützen	Märkte stören	Einhaltung erleichtern

Es wurden fünf Kategorien entwickelt – Reduzierung der Häufigkeit von Gelegenheiten; wahrgenommenen Aufwand erhöhen; wahrgenommenes Risiko erhöhen, erwartete Belohnung verringern, Ausflüchte eliminieren – die 20 situative Präventionsmaßnahmen gegen Cyberkriminalität enthalten. Die *Reduzierung der Häufigkeit von Gelegenheiten* umfasst das Nicht-Vorstellen der Ziele (z. B. kein Zugang zu Chats), das Identifizieren der Risikozonen (z. B. Informationskampagnen über die Risiken in sozialen Netzwerken), die Dekontamination/Beseitigung von Rückständen und das Trennen der Ziele (z. B. durch die Schaffung untergeordneter, lokaler Sicherheitsnetzwerke). Die *Erhöhung des wahrgenommenen Aufwands* umfasst die Kontrolle des Systemzugangs (z. B. durch Updates des Betriebssystems, Passwörter und Lizenzen); die Feststellung und Verhinderung von Angriffen (z. B. Antiviren-Software, Anti-Spyware, Anti-Spam-Maßnahmen); das Umlenken der Täter (z. B. Entfernung illegaler Inhalte; Zugangsbeschränkungen für[109] spezifische IP-Adressen); Kontrolle von Waffen/Werkzeugen. Die *Erhöhung des wahrgenommenen Risikos* beruht auf der Ausweitung der Bewachung/Überwachung (z. B. durch Dritte), Reduzierung der Anonymität (z. B. Identifizierung von IP-Adressen; Registrierung in *Web*-Foren; Nutzeridentifikationssysteme), Verstärkung formeller Überwachung (z. B. Teams, die auf die Untersuchung von Cyberkriminalität spezialisiert sind) und Unterstützung der natürlichen Überwachung (z. B. Verbesserung von IP-Identifizierungssystemen). Die vierte Kategorie beinhaltet: das Verbergen von Zielen (z. B. durch die Verwendung von Verschlüsselungssystemen; Verbergen persönlicher Daten in sozialen Netzwerken); das Entfernen von Zielen (z. B. durch die Verwendung externer Festplatten; Verwendung alternative Zahlungssysteme wie *PayPal*; Nachrichtenanfragen unbekannter Personen ignorieren); Entfernung der Vorteile; Störung der Märkte (z. B. durch die Kontrolle von Webseiten, von denen direkt Inhalte heruntergeladen werden können). Das *Eliminieren der Ausflüchte* umfasst: das Aufstellen von Regeln (z. B. die Harmonisierung der Gesetzgebung auf internationaler Ebene); das Aufstellen von Regeln (z. B. Privatsphäre-Einstellungen in sozialen Netzwerken); die Stärkung des moralischen Bewusstseins (z. B. Aufklärung über geistiges Eigentum); und Erleichterung der Einhaltung (z. B. legale Hacking-Wettbewerbe; Stärkung von Open-Software-Angeboten).

[109] IP bezeichnet die Internetprotokolladresse, eine Kennzeichnung bzw. ein Code, der jedem Gerät zugeordnet werden kann, der mit dem Computernetzwerk verbunden ist.

4. DIE WICHTIGE ROLLE DER PRÄVENTION IM KAMPF GEGEN CYBERKRIMINALITÄT

Die verfügbaren Nachweise für die Effizienz situativer Präventionstechniken im Kampf gegen Cyberkriminalität fokussieren sich auf die Erhöhung des Aufwands, zum Beispiel durch Kontroll- und Erkennungsmechanismen oder Softwares, und auf die Erhöhung des Risikos durch formelle Überwachungsmöglichkeiten. Die Erforschung der Wirksamkeit von Antivirenprogrammen bei der Erkennung und Verhinderung von Malware-Infektionen zeigt, dass die meisten Produkte solche Infektionen effizient feststellen und verhindern können (Brewer et al., 2019).

LITERATURVERZEICHNIS INTERNETQUELLEN

LITERATURVERZEICHNIS
INTERNETQUELLEN

LITERATURVERZEICHNIS – TEIL I

Agustina, J. R. (2015). Understanding cyber victimization: Digital architectures and the disinhibition effect. International Journal of Cyber Criminology, 9(1): 35-54.

APAV (2011). Manual crianças e jovens vítimas de violência: compreender, intervir e APAV (2011). Manual crianças e jovens vítimas de violência: compreender, intervir e prevenir. ISBN 978-972-8852-50-4. Lissabon: APAV.

APAV (2018). T@LK Handbook – online support for victims of crime. ISBN 978-972-8852-90-0. Lissabon: APAV.

APAV (2019). Manual CARE: apoio a crianças e jovens vítimas de violência sexual (2ª edição revista e aumentada). ISBN 978-972-8852-96-2. Lissabon: APAV.

Arafa, A. E., Mahmoud, O. E., & Senosy, S. A. (2015). The emotional impacts of different forms of cyberbullying victimization in Egyptian university students. Ägypten. J. Med. Sci, 36(2), 867-80.

Berelowitz, S., Firmin, C., Edwards, G., & Gulyurtlu, S. (2012). I thought I was the only one. The only one in the world. The Office of the Children's Commissioner's Inquiry into Child Sexual Exploitation In Gangs and Groups: Interim report. London: The Office of the Children's Commissioner in England.

Bossler, A. M., & Burruss, G. W. (2012). The general theory of crime and computer hacking: Low self-control hackers? In Cyber Crime: Concepts, Methodologies, Tools and Applications (pp. 1499-1527). IGI Global.

Cardoso, J., Ramos, C., Almeida, T., Gomes, A., Fernandes, A., & Ribeiro, R. (2018). 117 Cyber pornography use inventory-9: factor structure and psychometric properties in the Portuguese population. The Journal of Sexual Medicine, 15(7), S177.

Councill, B., & Heineman, G. T. (2001). Definition of a software component and its elements. Component-based software engineering: putting the pieces together, 5-19.

Cross, C., Richards, K., & Smith, R. G. (2016). Improving responses to online fraud vic-tims: An examination of reporting and support.

Das, S., & Nayak, T. (2013). Impact of cyber crime: Issues and challenges. International journal of engineering sciences & Emerging technologies, 6(2), 142-153.

Davies, E. L., Clark, J., & Roden, A. L. (2016). Self-Reports of Adverse Health Effects As-sociated with Cyberstalking and Cyberharassment: A Thematic Analysis of Victims' Lived Experiences.

De Kimpe, L., Ponnet, K., Walrave, M., Snaphaan, T., Pauwels, L., & Hardyns, W. (2020). Help, I need somebody: examining the antecedents of social support seeking among cybercrime victims. Computers in Human Behavior, 106310.

ECPAT, I. (2018). Towards a global indicator: on unidentified victms in child sexual ex-ploitation material. Ecpat Internacional: Bangkok, Thailand.

EU-Kommission. (2015). Special Eurobarometer 423: Cyber Security Report.

EUROPOL (2019). Internet organised crime threat assessment (IOCTA) 2019.

Gañán, C. H., Ciere, M., & van Eeten, M. (2017, October). Beyond the pretty penny: the Economic Impact of Cybercrime. In Proceedings of the 2017 New Security Para-digms Workshop (pp. 35-45).

Gao, J., Li, L., Kong, P., Bissyandé, T. F., & Klein, J. (2019, February). Should you consider adware as malware in your study? In 2019 IEEE 26th International Conference on Software Analysis, Evolution and Reengineering (SANER) (pp. 604-608). IEEE.

Goucher, W. (2010). Being a cybercrime victim. Computer Fraud & Security, 2010(10), 16-18.

Greijer, S., & Doek, J. (2016). Terminology guidelines for the protection of children from sexual exploitation and sexual abuse. Luxemburg: ECPAT International.

Hansen, J. V., Lowry, P. B., Meservy, R. D., & McDonald, D. M. (2007). Genetic programming for prevention of cyberterrorism through dynamic and evolving intrusion detection. Decision Support Systems, 43(4), 1362-1374.

Holt, T. J., & Bossler, A. M. (2008). Examining the applicability of lifestyle-routine activities theory for cybercrime victimization. Deviant Behavior, 30(1), 1-25.

Jahankhani, H., Al-Nemrat, A., & Hosseinian-Far, A. (2014). Cybercrime classification and characteristics. In Cyber Crime and Cyber Terrorism Investigator's Handbook (pp. 149-164). Syngress.

Jansen, J. & Leukfeldt, R. (2018). Coping with cybercrime victimization: an exploratory study into impact and change. Journal of Qualitative Criminal Justice and Criminology, 2: 205-227.

Kanayamaa, T. (2017). Impact of Cybercrime in Japan - Findings of Cybercrime Victimization Survey. Sociology, 7(6), 331-340.

Kansagra, D., Kumhar, M., & Jha, D. (2016). Ransomware: A Threat to Cyber security. CS Journals, 7(1).

Kienzle, D. M., & Elder, M. C. (2003, October). Recent worms: a survey and trends. In Proceedings of the 2003 ACM workshop on Rapid malcode (pp. 1-10).

Kigerl, A. (2012). Routine activity theory and the determinants of high cybercrime countries. Social Science Computer Review, 30(4), 470-486.

Koops, B. J. (2010). The internet and its opportunities for cybercrime. Transnational Criminology Manual, M. Herzog-Evans, ed, 1, 735-754.

Kratchman, S., Smith, J. L., & Smith, M. (2008). The Perpetration and Prevention of Cybercrimes. Verfügbar über SSRN 1123743.

Leukfeldt, E. R. (2015). Organised cybercrime and social opportunity structures: A proposal for future research directions. The European Review of Organised Crime, 2(2), 91-103.

Leukfeldt, E. R., Notté, R. J., & Malsch, M. (2020). Exploring the Needs of Victims of Cyber-dependent and Cyber-enabled Crimes. Victims & Offenders, 15(1), 60-77.

Louderback, E. R., & Antonaccio, O. (2017). Exploring cognitive decision-making processes, computer-focused cyber deviance involvement and victimization: The role of thought-fully reflective decision-making. Journal of research in crime and delinquency, 54(5), 639-679.

Maia, R. L., Nunes, L. M., Caridade, S., Sani, A. I., Estrada, R., Nogueira, C., Fernandes, H. & Afonso, L. (2016). Dicionário - Crime, Justiça e Sociedade (1.ª ed.). Lissabon: Edições Sílabo.

Maimon, D., & Louderback, E. R. (2019). Cyber-dependent crimes: An interdisciplinary review. Annual Review of Criminology, 2:191-216.

Maran, D. A., & Begotti, T. (2019). Prevalence of Cyberstalking and Previous Offline Victimization in a Sample of Italian University Students. Social Sciences, 8(1).

Marcum, C. D., Higgins, G. E., Ricketts, M. L., & Wolfe, S. E. (2014). Hacking in high school: Cybercrime perpetration by juveniles. Deviant Behavior, 35(7), 581-591.

Martellozzo, E., & Jane, E. A. (Eds.). (2017). Cybercrime and its victims. Taylor & Francis.

McGonagle, T. (2013). The Council of Europe against online hate speech: Conundrums and challenges. In Expert paper. Belgrad: Council of Europe Conference of Ministers responsible for Media and Information Society.

McNeeley, S. (2015). Lifestyle-routine activities and crime events. Journal of Contemporary Criminal Justice, 31(1), 30-52.

Modic, D., & Anderson, R. (2015). It's All Over but the Crying: The Emotional and Fi-nancial Impact of Internet Fraud. IEEE Security & Privacy, 13(5), 99-103.

Moitra, S. D. (2004). Cybercrime: Towards an assessment of its nature and impact. International Journal of Comparative and Applied Criminal Justice, 28(2), 105-123.

Näsi, M., Oksanen, A., Keipi, T., & Räsänen, P. (2015). Cybercrime victimization among young people: a multi-nation study. Journal of Scandinavian Studies in Criminology and Crime Prevention, 16(2), 203-210.

Neghina, D. E., & Scarlat, E. (2013). Managing information technology security in the context of cyber crime trends. International journal of computers communications & control, 8(1), 97-104.

Ngo, F. T., & Paternoster, R. (2011). Cybercrime Victimization: An examination of Individual and Situational level factors. International Journal of Cyber Criminology, 5(1).

Nykodym, N., Taylor, R., & Vilela, J. (2005). Criminal profiling and insider cyber crime. Computer Law & Security Review, 21(5), 408-414.

Overvest, B., & Straathof, B. (2015). What drives cybercrime? Empirical evidence from DDoS attacks (No. 306. rdf). CPB Netherlands Bureau for Economic Policy Analysis.

Patel, R. D., & Singh, D. K. (2013). Credit card fraud detection & prevention of fraud using genetic algorithm. International Journal of Soft Computing and Engineering, 2(6), 292-294.

Peterson, J., & Densley, J. (2017). Cyber violence: What do we know and where do we go from here? Aggression and violent behavior, 34, 193-200.

Phillips, E. (2015). Empirical Assessment of Lifestyle-Routine Activity and Social Learn-ing Theory on Cybercrime Offending.

Poong, Y., Zaman, K. U., & Talha, M. (2006, August). E-commerce today and tomorrow: a truly generalized and active framework for the definition of electronic commerce. In Proceedings of the 8th international conference on Electronic commerce: The new e-commerce: innovations for conquering current barriers, obstacles and limitations to conducting successful business on the internet (pp. 553-557).

Rathi, M., & Pareek, V. (2013). Spam mail detection through data mining - A comparative performance analysis. International Journal of Modern Education and Computer Science, 5(12), 31.

Reep-van den Bergh, C. M., & Junger, M. (2018). Victims of cybercrime in Europe: a review of victim surveys. Crime science, 7: 1-15.

Saban, K. A., McGivern, E., & Saykiewicz, J. N. (2002). A critical look at the impact of cybercrime on consumer Internet behavior. Journal of Marketing Theory and Practice, 10(2), 29-37.

Saridakis, G., Benson, V., Ezingeard, J. N., & Tennakoon, H. (2016). Individual information security, user behaviour and cyber victimisation: An empirical study of social networking users. Technological Forecasting and Social Change, 102, 320-330.

Seifert, C., Stokes, J., Lu, L., Heckerman, D., Colcernian, C., Parthasarathy, S., & Santhanam, N. (2015). U.S. Patent No. 9,130,988. Washington, DC: U.S. Patent and Trademark Office.

Sharpe, J., & Self, R. (2015). Computers for Everyone. Computers for Everyone, 1(1).

Sigurjonsdottir, S. (2013). Consequences of victims' mental health after Internet-initiated sexual abuse; a sexual grooming case in Sweden.

Smith, A. D. (2004). Cybercriminal impacts on online business and consumer confidence. Online Information Review, 28(3), 224-234.

Suler, J. (2004). The online disinhibition effect. CyberPsychology & Behavior, 3: 321-326.

Van Wilsem, J. (2011). Worlds tied together? Online and non-domestic routine activities and their impact on digital and traditional threat victimization. European Journal of Criminology, 8(2), 115-127.

World Health Organization. (2017). Responding to children and adolescents who have been sexually abused: WHO clinical guidelines. ISBN 978-92-4-155014-7. Genf: World Health Organization.

Yar, M. & Steinmetz, K. F. (2019). Cybercrime and society (3rd edition). ISBN 978-1-5264-4065-5. London: SAGE.

Yucedal, B. (2010). Victimization in cyberspace: An application of Routine Activity and Lifestyle Exposure theories (Doctoral dissertation, Kent State University).

LITERATURVERZEICHNIS – TEIL II

Agustina, J. R. (2015). Understanding cyber victimization: Digital architectures and the disinhibition effect. *International Journal of Cyber Criminology, 9*(1): 35-54.

Ajzen, I. (1991). The theory of planned behavior. *Organizational behavior and human decision processes, 50*(2), 179-211.

Al-Ali, A. A., Nimrat, A., & Benzaid, C. (2018). Combating Cyber Victimisation: Cybercrime Prevention. In *Cyber Criminology* (pp. 325-339). Springer, Cham.

Alexy, E. M., Burgess, A. W., Baker, T., & Smoyak, S. A. (2005). Perceptions of *ciber--stalking* among college students. *Brief treatment and crisis intervention*, 5(3), 279.

Amador, N. J. R. (2012). *Cibercrime em Portugal: Trajetórias e Perspetivas de Futuro* (Doctoral dissertation).

Ang, R. P. (2015). Adolescent *ciber-bullying*: A review of characteristics, prevention and intervention strategies. *Aggression and violent behavior, 25*, 35-42.

APAV (2011). *Manual crianças e jovens vítimas de violência: compreender, intervir e prevenir.* ISBN 978-972-8852-50-4. Lisboa: APAV.

APAV (2013). *Manual Unisexo – para o atendimento a vítimas adultas de violência sexual.* Lisboa: APAV.

APAV (2017). *T@LK Handbook – Online Support for Victims of Crime.* ISBN 978-972-8852-90-0. Lisboa: APAV.

APAV (2018). *Manual ódio nunca mais: apoio a vítimas de crimes de ódio.* ISBN 978-972-8852-91-7. Lisboa: APAV.

APAV (2019). *Manual CARE: apoio a crianças e jovens vítimas de violência sexual* (2ª edição revista e aumentada). ISBN 978-972-8852-96-2. Lisboa: APAV.

APAV (2019b). *Manual EMAV : atendimento e encaminhamento de vítimas de violência doméstica e de género : procedimentos & roteiro de recursos*. ISBN 978-989-54322-2-6. Lisboa: APAV.

Arafa, A. E., Mahmoud, O. E., & Senosy, S. A. (2015). The emotional impacts of different forms of *ciber-bullying* victimization in Egyptian university students. Egypt. J. Med. Sci, 36(2), 867-80.

Askerniya, I. How best to protect the user-individuals in Moscow from cyber crime attacks.

Balkin, J., Grimmelmann, J., Katz, E., Kozlovski, N., Wagman, S., & Zarsky, T. (Eds.). (2007). *Cybercrime: digital cops in a networked environment* (Vol. 4). NYU Press.

Baskerville, R., Spagnoletti, P., & Kim, J. (2014). Incident-centered information security: Managing a strategic balance between prevention and response. Information & management, 51(1), 138-151.

Berelowitz, S., Firmin, C., Edwards, G., & Gulyurtlu, S. (2012). I thought I was the only one. The only one in the world. *The Office of the Children's Commissioner's Inquiry into Child Sexual Exploitation In Gangs and Groups: Interim report. London: The Office of the Children's Commissioner in England.*

Boehmer, J., LaRose, R., Rifon, N., Alhabash, S., & Cotten, S. (2015). Determinants of online safety behaviour: towards an intervention strategy for college students. *Behaviour & Information Technology, 34*(10), 1022-1035.

Bossler, A. M., & Burruss, G. W. (2012). The general theory of crime and computer hacking: Low self-control hackers? In Cyber Crime: Concepts, Methodologies, Tools and Applications (pp. 1499-1527). IGI Global.

Brewer, R., de Vel-Palumbo, M., Hutchings, A., Holt, T., Goldsmith, A., & Maimon, D. (2019). *Cybercrime Prevention: Theory and Applications.* Springer Nature.

Brown, C. F., Demaray, M. K., Tennant, J. E., & Jenkins, L. N. (2017). Cyber victimization in high school: Measurement, overlap with face-to-face victimization, and associations with social–emotional outcomes. *School psychology review, 46*(3), 288-303.

Buchanan, T., Paine, C., Joinson, A. N., & Reips, U. D. (2007). Development of measures of *online* privacy concern and protection for use on the Internet. *Journal of the American society for information science and technology, 58*(2), 157-165.

Burns, S., & Roberts, L. (2013). Applying the theory of planned behaviour to predicting online safety behaviour. *Crime Prevention and Community Safety, 15*(1), 48-64.

Callahan, A., & Inckle, K. (2012). Cybertherapy or psychobabble? A mixed methods study of online emotional support. *British Journal of Guidance & Counselling, 40*(3), 261-278.

Cardoso, J., Ramos, C., Almeida, T., Gomes, A., Fernandes, A., & Ribeiro, R. (2018). 117 Cyber pornography use inventory-9: factor structure and psychometric properties in the Portuguese population. The Journal of Sexual Medicine, 15(7), S177.

Chisholm, J. F. (2014). Review of the status of ciber-bullying and ciber-bullying prevention. *Journal of Information Systems Education, 25*(1), 77.

Cornish, D. B., & Clarke, R. V. (2003). Opportunities, precipitators and criminal decisions: A reply to Wortley's critique of situational crime prevention. *Crime prevention studies, 16*, 41-96.

Councill, B., & Heineman, G. T. (2001). Definition of a software component and its elements. Component-based software engineering: putting the pieces together, 5-19.

Cross, C., Richards, K., & Smith, R. G. (2016). Improving responses to *online* fraud victims: An examination of reporting and support.

Cross, D., Shaw, T., Hadwen, K., Cardoso, P., Slee, P., Roberts, C., & Barnes, A. (2016). Longitudinal impact of the Cyber Friendly Schools program on adolescents' *ciber-bullying* behavior. *Aggressive behavior, 42*(2), 166-180.

Das, S., & Nayak, T. (2013). Impact of cyber crime: Issues and challenges. International journal of engineering sciences & Emerging technologies, 6(2), 142-153.

Dashora, K. (2011). Cyber crime in the society: Problems and preventions. *Journal of Alternative Perspectives in the social sciences, 3*(1), 240-259.

Davies, E. L., Clark, J., & Roden, A. L. (2016). Self-Reports of Adverse Health Effects Associated with *Ciber-stalking* and Cyberharassment: A Thematic Analysis of Victims' Lived Experiences.

De Kimpe, L., Ponnet, K., Walrave, M., Snaphaan, T., Pauwels, L., & Hardyns, W. (2020). Help, I need somebody: examining the antecedents of social support seeking among cybercrime victims. *Computers in Human Behavior*, 106310.

De Vignemont, F., & Singer, T. (2006). The empathic brain: how, when and why?. *Trends in cognitive sciences, 10*(10), 435-441.

Dooley, J. J., Gradinger, P., Strohmeier, D., Cross, D., & Spiel, C. (2010). Cyber-victimisation: The association between help-seeking behaviours and self-reported emotional symptoms in Australia and Austria. *Journal of Psychologists and Counsellors in Schools, 20*(2), 194-209.

ECPAT, I. (2018). Towards a global indicator: on unidentified victims in child sexual exploitation material. Ecpat International: Bangkok, Thailand.

Edirisuriya, M. A. V. S., & Liyanage, L. S. (2016). Application of Protective Motivation Theory in cyber safety context: Human factor in risk mitigation.

EU Commission. (2015). Special Eurobarometer 423: Cyber Security Report.

EUROPOL (2019). Internet organised crime threat assessment (IOCTA) 2019.

Finn, J., & Banach, M. (2000). Victimization online: The downside of seeking human services for women on the Internet. *CyberPsychology & Behavior, 3*(5), 785-796.

Gañán, C. H., Ciere, M., & van Eeten, M. (2017, October). Beyond the pretty penny: the Economic Impact of Cybercrime. In Proceedings of the 2017 New Security Paradigms Workshop (pp. 35-45).

Gao, J., Li, L., Kong, P., Bissyandé, T. F., & Klein, J. (2019, February). Should you consider adware as malware in your study? In 2019 IEEE 26th International Conference on Software Analysis, Evolution and Reengineering (SANER) (pp. 604-608). IEEE.

Goucher, W. (2010). Being a cybercrime victim. Computer Fraud & Security, 2010(10), 16-18.

Grabosky, P. (2007). Requirements of prosecution services to deal with cyber crime. *Crime, law and social change, 47*(4-5), 201-223.

Greijer, S., & Doek, J. (2016). Terminology guidelines for the protection of children from sexual exploitation and sexual abuse. Luxembourg: ECPAT International.

Hansen, J. V., Lowry, P. B., Meservy, R. D., & McDonald, D. M. (2007). Genetic programming for prevention of cyberterrorism through dynamic and evolving intrusion detection. Decision Support Systems, 43(4), 1362-1374.

Hinduja, S., & Kooi, B. (2013). Curtailing cyber and information security vulnerabilities through situational crime prevention. *Security journal, 26*(4), 383-402.

Holt, T. J., & Bossler, A. M. (2008). Examining the applicability of lifestyle-routine activities theory for cybercrime victimization. Deviant Behavior, 30(1), 1-25.

Holt, T. J., & Bossler, A. M. (2015). Cybercrime in progress: *Theory and prevention of technology-enabled offenses*. Routledge.

Jäger, T., Amado, J., Matos, A., & Pessoa, T. (2010). Analysis of experts' and trainers' views on *ciber-bullying. Journal of Psychologists and Counsellors in Schools, 20*(2), 169-181.

Jahankhani, H., Al-Nemrat, A., & Hosseinian-Far, A. (2014). Cybercrime classification and characteristics. In Cyber Crime and Cyber Terrorism Investigator's Handbook (pp. 149-164). Syngress.

Jansen, J. & Leukfeldt, R. (2018). Coping with cybercrime victimization: an exploratory study into impact and change. Journal of Qualitative Criminal Justice and Criminology, 2: 205-227.

Kaakinen, M., Keipi, T., Räsänen, P., & Oksanen, A. (2018). Cybercrime victimization and subjective well-being: An examination of the buffering effect hypothesis among adolescents and young adults. *Cyberpsychology, Behavior, and Social Networking, 21*(2), 129-137.

Kanayamaa, T. (2017). Impact of Cybercrime in Japan - Findings of Cybercrime Victimization Survey. Sociology, 7(6), 331-340.

Kaniasty, K., & Norris, F. H. (1992). Social support and victims of crime: Matching event, support, and outcome. *American journal of community psychology, 20*(2), 211-241.

Kansagra, D., Kumhar, M., & Jha, D. (2016). Ransomware: A Threat to Cyber security. CS Journals, 7(1).

Kienzle, D. M., & Elder, M. C. (2003, October). Recent worms: a survey and trends. In Proceedings of the 2003 ACM workshop on Rapid malcode (pp. 1-10).

Kigerl, A. (2012). Routine activity theory and the determinants of high cybercrime countries. Social Science Computer Review, 30(4), 470-486.

Koops, B. J. (2010). The internet and its opportunities for cybercrime. Transnational Criminology Manual, M. Herzog-Evans, ed., 1, 735-754.

Kratchman, S., Smith, J. L., & Smith, M. (2008). The Perpetration and Prevention of Cybercrimes. Available at SSRN 1123743.

LaRose, R., & Rifon, N. J. (2007). Promoting i-safety: effects of privacy warnings and privacy seals on risk assessment and *online* privacy behavior. *Journal of Consumer Affairs*, 41(1), 127-149.

Lee, D., Larose, R., & Rifon, N. (2008). Keeping our network safe: a model of *online* protection behaviour. *Behaviour & Information Technology, 27*(5), 445-454.

Leukfeldt, E. R. (2015). Organised cybercrime and social opportunity structures: A proposal for future research directions. The European Review of Organised Crime, 2(2), 91-103.

Leukfeldt, E. R., Notté, R. J., & Malsch, M. (2020). Exploring the Needs of Victims of Cyber-dependent and Cyber-enabled Crimes. Victims & Offenders, 15(1), 60-77.

Ljungwald, C., & Svensson, K. (2007). Crime Victims and the Social Services: Social Workers' Viewpoint. *Journal of Scandinavian Studies in Criminology and Crime Prevention, 8*(2), 138-156.

Louderback, E. R., & Antonaccio, O. (2017). Exploring cognitive decision-making processes, computer-focused cyber deviance involvement and victimization: The role of thoughtfully reflective decision-making. Journal of research in crime and delinquency, 54(5), 639-679.

Lwin, M. O., Ang, R. P., & Liu, C. (2013). Cognitive, personality, and social factors associated with adolescents' *online* personal information disclosure.

Lwin, M. O., Li, B., & Ang, R. P. (2012). Stop bugging me: An examination of adolescents' protection behavior against online harassment. *Journal of adolescence, 35*(1), 31-41.

Maia, R. L., Nunes, L. M., Caridade, S., Sani, A. I., Estrada, R., Nogueira, C., Fernandes, H. & Afonso, L. (2016). *Dicionário - Crime, Justiça e Sociedade* (1.ª ed.). Lisboa: Edições Sílabo.

Maimon, D., & Louderback, E. R. (2019). Cyber-dependent crimes: An interdisciplinary review. Annual Review of Criminology, 2:191-216.

Mallen, M. J., Vogel, D. L., & Rochlen, A. B. (2005). The practical aspects of *online* counseling: Ethics, training, technology, and competency. *The Counseling Psychologist, 33*(6), 776-818.

Maran, D. A., & Begotti, T. (2019). Prevalence of *Ciber-stalking* and Previous *Offline* Victimization in a Sample of Italian University Students. Social Sciences, 8(1).

Marcum, C. D., Higgins, G. E., Ricketts, M. L., & Wolfe, S. E. (2014). Hacking in high school: Cybercrime perpetration by juveniles. Deviant Behavior, 35(7), 581-591.

Marczak, M., & Coyne, I. (2010). *Ciber-bullying* at school: Good practice and legal aspects in the United Kingdom. *Journal of Psychologists and Counsellors in Schools, 20*(2), 182-193.

Marques, P. P. L. D. C. (2013). *Informática forense: recolha e preservação da prova digital* (Doctoral dissertation).

Martellozzo, E., & Jane, E. A. (Eds.). (2017). Cybercrime and its victims. Taylor & Francis.

Martins, M. J. D., Simão, A. M. V., Freire, I., Caetano, A. P., & Matos, A. (2017). Cyber-victimization and cyber-aggression among Portuguese adolescents: The relation to family support and family rules. In *Violence and society: Breakthroughs in research and practice* (pp. 134-149). IGI Global.

Matos, A., Pessoa, T., Amado, J., & Jäger, T. (2011). Agir contra o *ciber-bullying*–manual de formação. *Literacia, Media e Cidadania*, 183-196.

McCann, I. L., & Pearlman, L. A. (1990). Vicarious traumatization: A framework for understanding the psychological effects of working with victims. *Journal of Traumatic Stress, 3*(1), 131–149.

McGonagle, T. (2013). The Council of Europe against online hate speech: Conundrums and challenges. In Expert paper. Belgrade: Council of Europe Conference of Ministers responsible for Media and Information Society.

McNeeley, S. (2015). Lifestyle-routine activities and crime events. Journal of Contemporary Criminal Justice, 31(1), 30-52.

Mesch, G. S. (2009). Parental mediation, online activities, and *ciber-bullying. CyberPsychology & Behavior, 12*(4), 387-393.

Modic, D., & Anderson, R. (2015). It's All Over but the Crying: The Emotional and Financial Impact of Internet Fraud. *IEEE Security & Privacy, 13*(5), 99-103.

Moitra, S. D. (2004). Cybercrime: Towards an assessment of its nature and impact. International Journal of Comparative and Applied Criminal Justice, 28(2), 105-123.

Näsi, M., Oksanen, A., Keipi, T., & Räsänen, P. (2015). Cybercrime victimization among young people: a multi-nation study. Journal of Scandinavian Studies in Criminology and Crime Prevention, 16(2), 203-210.

Neghina, D. E., & Scarlat, E. (2013). Managing information technology security in the context of cyber crime trends. International journal of computers communications & control, 8(1), 97-104.

Ngo, F. T., & Paternoster, R. (2011). Cybercrime Victimization: An examination of Individual and Situational level factors. International Journal of Cyber Criminology, 5(1).

Notar, C. E., Padgett, S., & Roden, J. (2013). *Ciber-bullying*: Resources for Intervention and Prevention. *Universal Journal of Educational Research, 1*(3), 133-145.

Nykodym, N., Taylor, R., & Vilela, J. (2005). Criminal profiling and insider cyber crime. Computer Law & Security Review, 21(5), 408-414.

Overvest, B., & Straathof, B. (2015). What drives cybercrime? Empirical evidence from DDoS attacks (No. 306. rdf). CPB Netherlands Bureau for Economic Policy Analysis.

Öztürk, E., & Akcan, G. (2016). Preventing and Coping Strategies for Cyber Bullying and Cyber Victimization. *International Journal of Information and Communication Engineering, 10*(5), 1771-1774.

Palladino, B. E., Nocentini, A., & Menesini, E. (2016). Evidence-based intervention against bullying and *ciber-bullying*: Evaluation of the NoTrap! program in two independent trials. *Aggressive behavior, 42*(2), 194-206.

Patel, R. D., & Singh, D. K. (2013). Credit card fraud detection & prevention of fraud using genetic algorithm. International Journal of Soft Computing and Engineering, 2(6), 292-294.

Pessoa, T., da Mota Matos, A. P., Amado, J., & Jäger, T. (2011). *Ciber-bullying*: do diagnóstico de necessidades à construção de um manual de formação. *Pedagogía social: revista interuniversitaria*, (18), 57-70.

Peterson, J., & Densley, J. (2017). Cyber violence: What do we know and where do we go from here? Aggression and violent behavior, 34, 193-200.

Phillips, E. (2015). Empirical Assessment of Lifestyle-Routine Activity and Social Learning Theory on Cybercrime Offending.

Poong, Y., Zaman, K. U., & Talha, M. (2006, August). E-commerce today and tomorrow: a truly generalized and active framework for the definition of electronic commerce. In Proceedings of the 8th international conference on Electronic commerce: The new e-commerce: innovations for conquering current barriers, obstacles and limitations to conducting successful business on the internet (pp. 553-557).

Poulin, F., Nadeau, K., & Scaramella, L. V. (2012). The role of parents in young adolescents' competence with peers: An observational study of advice giving and intrusiveness. *Merrill-Palmer Quarterly (1982-)*, 437-462.

Rathi, M., & Pareek, V. (2013). Spam mail detection through data mining-A comparative performance analysis. International Journal of Modern Education and Computer Science, 5(12), 31.

Reep-van den Bergh, C. M., & Junger, M. (2018). Victims of cybercrime in Europe: a review of victim surveys. Crime science, 7: 1-15.

Reyns, B. W. (2010). A situational crime prevention approach to *ciber-stalking* victimization: Preventive tactics for Internet users and *online* place managers. *Crime Prevention and Community Safety, 12*(2), 99-118.

Reyns, B. W., & Henson, B. (2016). The thief with a thousand faces and the victim with none: Identifying determinants for *online* identity theft victimization with routine activity theory. *International journal of offender therapy and comparative criminology, 6*0(10), 1119-1139.

Reyns, B. W., Randa, R., & Henson, B. (2016). Preventing crime *online*: Identifying determinants of online preventive behaviors using structural equation modeling and canonical correlation analysis. *Crime Prevention and Community Safety, 18*(1), 38-59.

Ribeiro, M. D. C. F. (2015). *Cibercrime e Prova Digital* (Doctoral dissertation).

Richardson, J., & Milovidov, E. (2019). *Digital citizenship education handbook: Being online, well-being online, and rights online*. Council of Europe.

Saavedra, R. & Machado, C. (2010). Pevenção universal da violência em contexto escolar. In C. Machado (Coord.), *Vitimologia: das novas abordagens teóricas às novas práticas de intervenção* (pp. 137-167). Braga: Psiquilíbrios Edições.

Saban, K. A., McGivern, E., & Saykiewicz, J. N. (2002). A critical look at the impact of cybercrime on consumer Internet behavior. Journal of Marketing Theory and Practice, 10(2), 29-37.

Sampson, R., Eck, J. E., & Dunham, J. (2010). Super controllers and crime prevention: A routine activity explanation of crime prevention success and failure. *Security Journal, 23*(1), 37-51.

Santos, A. F. C. (2016). *O cibercrime: desafios e respostas do direito* (Doctoral dissertation).

Saridakis, G., Benson, V., Ezingeard, J. N., & Tennakoon, H. (2016). Individual information security, user behaviour and cyber victimisation: An empirical study of social networking users. *Technological Forecasting and Social Change, 102*, 320-330.

Seifert, C., Stokes, J., Lu, L., Heckerman, D., Colcernian, C., Parthasarathy, S., & Santhanam, N. (2015). U.S. Patent No. 9,130,988. Washington, DC: U.S. Patent and Trademark Office.

Sharpe, J., & Self, R. (2015). Computers for Everyone. Computers for Everyone, 1(1).

Sigurjonsdottir, S. (2013). Consequences of victims' mental health after Internet--initiated sexual abuse; a sexual grooming case in Sweden.

Skorodumov, B. I., Skorodumova, O. B., & Matronina, L. F. (2015). Research of human factors in information security. *Modern Applied Science, 9*(5), 287.

Smallbone, S., & Wortley, R. (2017). 8 Preventing Child Sexual Abuse *Online. Online Risk to Children: Impact, Protection and Prevention*, 143.

Smith, A. D. (2004). Cybercriminal impacts on online business and consumer confidence. *Online* Information Review, 28(3), 224-234.

Suler, J. (2004). The *online* disinhibition effect. CyberPsychology & Behavior, 3: 321-326.

Tanrikulu, I. (2018). *Ciber-bullying* prevention and intervention programs in schools: A systematic review. *School psychology international, 39*(1), 74-91.

van der Wagen, W., & Pieters, W. (2018). The hybrid victim: Re-conceptualizing high-tech cyber victimization through actor-network theory. *European Journal of Criminology,* 1477370818812016.

van Wilsem, J. (2011). Worlds tied together? Online and non-domestic routine activities and their impact on digital and traditional threat victimization. *European Journal of Criminology, 8*(2), 115-127.

Van Wilsem, J. (2013). Hacking and harassment—do they have something in common? Comparing risk factors for online victimization. *Journal of Contemporary Criminal Justice, 29*(4), 437-453.

Wedlock, E., & Tapley, J. D. (2016). What works in supporting victims of crime: A rapid evidence assessment.

Winkel, F. W. (1991). Police, victims, and crime prevention: Some research-based recommendations on victim-orientated interventions. *The British Journal of Criminology, 31*(3), 250-265.

Wolak, J., Finkelhor, D., Mitchell, K. J., & Ybarra, M. L. (2010). *Online* "predators" and their victims: Myths, realities, and implications for prevention and treatment.

World Health Organization. (2017). Responding to children and adolescents who have been sexually abused: WHO clinical guidelines. ISBN 978-92-4-155014-7. Geneva: World Health Organization.

Wright, J. (2002). *Online* counselling: Learning from writing therapy. *British Journal of Guidance and Counselling, 30*(3), 285-298.

Wright, M. F. (2015). Cyber Victimization: A New Kind of Victimization. *Nova Science Publishers, Inc.*

Wright, M. F. (2018). Ciber-stalking victimization, depression, and academic performance: The role of perceived social support from parents. *Cyberpsychology, Behavior, and Social Networking, 21*(2), 110-116.

Yar, M. & Steinmetz, K. F. (2019). Cybercrime and society (3rd edition). ISBN 978-1-5264-4065-5. London: SAGE.

Yucedal, B. (2010). Victimization in cyberspace: An application of Routine Activity and Lifestyle Exposure theories (Doctoral dissertation, Kent State University).

INTERNETQUELLEN

TEIL I

https://www.met.police.uk/advice/advice-and-information/fa/fraud/personal-fraud/online-shopping/

https://www.scamwatch.gov.au/types-of-scams/dating-romance

https://www.kaspersky.com/blog/online-dating-report/

https://www.cncs.gov.pt/recursos/glossario/

https://www.innocentlivesfoundation.org/gaming-and-grooming-how-minecraft-and-fortnite-could-be-dangerous/

https://articles.forensicfocus.com/2019/12/17/investigating-nonconsensual-intimate-image-sharing/

https://apav.pt/cibercrime/

https://techterms.com/definition/hardware

7159/1/17 REV 1 DCL 1 Evaluation Report on the seventh round of mutual evaluations "The practical implementation and operation of European policies on prevention and combating cybercrime" - Report on Germany, Brussels, 19 May 2017

https://data.consilium.europa.eu/doc/document/ST-7159-2017-REV-1-COR-1-DCL-1/en/pdf

https://www.gesetze-im-internet.de/bdsg_2018/BJNR209710017.html

https://www.gesetze-im-internet.de/tkg_2004/

https://www.gesetze-im-internet.de/tmg/BJNR017910007.html

https://ec.europa.eu/anti-trafficking/sites/antitrafficking/files/criminal_code_germany_en_1.pdf

TEIL II

https://dre.pt/legislacao-consolidada/-/lc/34520775/view

http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=775&tabela=leis

http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=199&tabela=leis

https://www.met.police.uk/advice/advice-and-information/fa/fraud/personal-fraud/online-shopping/

https://www.scamwatch.gov.au/types-of-scams/dating-romance

https://www.kaspersky.com/blog/online-dating-report/

https://www.cncs.gov.pt/recursos/glossario/

https://www.innocentlivesfoundation.org/gaming-and-grooming-how-minecraft-and-fortnite-could-be-dangerous/

https://articles.forensicfocus.com/2019/12/17/investigating-nonconsensual-intimate-image-sharing/

https://apav.pt/cibercrime/

https://techterms.com/definition/hardware

https://data.consilium.europa.eu/doc/document/ST-7159-2017-REV-1-COR-1-DCL-1/en/pdf

https://www.gesetze-im-internet.de/bdsg_2018/BJNR209710017.html

https://www.gesetze-im-internet.de/tkg_2004/

https://www.gesetze-im-internet.de/tmg/BJNR017910007.html

https://ec.europa.eu/anti-trafficking/sites/antitrafficking/files/criminal_code_germany_en_1.pdf

ROAR
empowering
victims of
cybercrime

APAV
associação portuguesa de
Apoio à Vítima

Diese Veröffentlichung wurde durch den Fonds für die innere Sicherheit der Europäischen Union — Polizei finanziert

MINISTÉRIO PÚBLICO
PORTUGAL
PROCURADORIA-GERAL DA REPÚBLICA

WEISSER RING
Wir helfen Kriminalitätsopfern.

ACTEDO

altice

ISBN:
978-989-53116-7-5