1. Formen der Bedrohung von Cyberkriminalität

Gina Rosa Wollinger, Arne Dreißigacker, Bennet Simon von Skarczinski

Inhaltsübersicht

1.1 Einleitung

Fast täglich berichten Medien über Vorfälle im Bereich Cyberkriminalität. Neben großen Unternehmen sind dabei auch kleine Firmen und Privatnutzer betroffen, ebenso wie kommunale Behörden. So musste die Stadtverwaltung von Neustadt am Rübenberge, eine Stadt mit rund 46000 Einwohnern in der Region Hannover, im September 2019 alle IT-Systeme abschalten.[1] Eine Schadsoftware hatte die Systeme angegriffen. Für die Bürger von Neustadt war die Stadtverwaltung daraufhin zunächst nur noch telefonisch oder vor Ort erreichbar. Selbst eineinhalb Wochen später konnten weder Autos angemeldet noch viele weitere Dienstleistungen der Stadtverwaltung genutzt werden.[2]

Im Fall von Neustadt war es ein Trojaner, der den Schaden ausgelöst hatte. Das Phänomen Cyberkriminalität weist jedoch noch viele weitere Bedrohungsformen und Angriffsarten auf. Ziel des vorliegenden Kapitels ist es, diese näher

1 https://www.ndr.de/nachrichten/niedersachsen/hannover_weser-leinegebiet/Trojaner-Neustadt-bleibt-bis-Freitag-offline,neustadt332.html (aufgerufen am 10.2.2020).

2 https://www.sueddeutsche.de/panorama/kriminalitaet-neustadt-am-ruebenberge-neustaedter-verwaltung-bleibt-nach-cyberangriff-lahmgelegt-dpa.urn-newsml-dpa-com-20090101-190916-99-901272 (aufgerufen am 10.2.2020).

darzustellen und damit zu skizzieren, was mit Cyberkriminalität gemeint ist. Dabei sind die Eingrenzung und Definition von Cyberkriminalität mit einigen Schwierigkeiten und Besonderheiten verbunden. Ein Grund hierfür ist, dass das Beschäftigungsfeld Cyberkriminalität durch eine Vielfalt an Akteuren gekennzeichnet ist. Neben unterschiedlichsten Gruppen von Betroffenen (Privatpersonen, Unternehmen, Staat usw.), sind auch die Täterstrukturen sehr heterogen (siehe dazu auch Kapitel 2 im vorliegenden Band). Ferner nehmen sich unterschiedliche Institutionen dem Thema an: Polizei-, Ermittlungsbehörden und Nachrichtendienste sind von staatlicher Stelle zu nennen, IT-Sicherheitsdienstleister bieten Beratungsangebote und Produkte an, um ihre Kunden vor Cyberkriminalität zu schützen. Zahlreiche Vereine und Verbände bilden Initiativen, um aufzuklären und für das Thema zu sensibilisieren. Wissenschaftler untersuchen Motivationen, so genannte Kill-Chains und Auswirkungen von Cyberangriffen und auch die Politik sieht Handlungsbedarf. Letzteres führte zu veränderten gesetzlichen Rahmenbedingungen, wie beispielsweise in Form des 2015 erlassenen *Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme* (so genanntes IT-Sicherheitsgesetz), und anderen politischen Initiativen wie die *Initiative IT-Sicherheit in der Wirtschaft*. Gefahren im Bereich der Informationssicherheit werden somit schon seit langer Zeit nicht nur in einem wissenschaftlichen Kontext, sondern verstärkt auch in der Fachpraxis, der Politik sowie der Öffentlichkeit diskutiert. So positiv es einerseits ist, dass das Thema der Gefahren im Zusammenhang mit dem Internet, der Digitalisierung und informationstechnischer Systeme breit aufgegriffen wird, so birgt dies andererseits jedoch auch spezifische Schwierigkeiten.

Zum einen führt das breite Spektrum des Phänomens Cyberkriminalität in Verbindung mit der Vielzahl unterschiedlicher Akteure zu einem Wildwuchs an Definitionen und Systematisierungen. Zahllose Versuche in der Literatur wurden unternommen, um Cybercrime in Taxonomien, Typologien, Klassifizierungen und Kategoriensystemen zu erfassen, aber wenige haben sich in der Praxis durchgesetzt (siehe *McGuire/Dowling*, 2013; *Paoli et al.*, 2018). Beispielsweise werden die Begriffe Informationssicherheit, IT-Sicherheit, Cyber-, Computer- bzw. Datensicherheit, Datenschutz und viele weitere synonym verwandt. Trotz aller Bemühungen fehlt es bislang an einer allgemeingültigen und konsensfähigen Definition und Systematisierung von Cyberkriminalität. Die uneinheitlichen Begriffsverwendungen und Begriffsverständnisweisen hemmen dabei die Transparenz und Vergleichbarkeit, beispielsweise in der statistischen Erfassung von Cyberkriminalität oder der Ausgestaltung von Richtlinien und Standards.

Zum anderen wird jedoch auch durch die mitunter unbegründete Uneinheitlichkeit interessierten Personen der Einstieg in das Thema erschwert. Die Schwierigkeit, einen Zugang zu dem Phänomenbereich Cyberkriminalität zu erlangen sowie Grundkenntnisse zu einem sicheren Umgang mit IT-Systemen zu erwerben, erscheint insbesondere aufgrund der Tatsache problematisch, dass digitale Programme und computerbasierte Prozesse stark in den Alltag und der Arbeitswelt des überwiegenden Teils der Bevölkerung integriert sind. Vor dem Hintergrund, dass die fortschreitende Digitalisierung und damit verbundene Sicherheitsrisiken eine gesellschaftliche Herausforderung darstellen,

kann und darf das Thema Cyberkriminalität bzw. die daraus resultierende Notwendigkeit für Informationssicherheit kein Expertenthema bleiben.

Ziel des vorliegenden Beitrags ist es, die verschiedenen Sichtweisen auf Cyberkriminalität sowie die Formen der Bedrohung auf informationstechnische Systeme undogmatisch zusammenzufassen, um dem Leser die Einordnung des Themas zu ermöglichen. Durch diese Orientierung ist es möglich, Unterschiede und Gemeinsamkeiten in weiterführender Literatur zu erkennen und kritisch zu würdigen. Dieser Beitrag stellt keine abschließende und nach wissenschaftlichen Kriterien erarbeitete Taxonomie[3] dar, sondern hat als Ziel, die Vielfalt von Cyberkriminalität punktuell aufzuzeigen und zu erläutern. Im Folgenden wird dazu zunächst eine Erläuterung verschiedener Begriffe im Zusammenhang mit „Cyber" und „Sicherheit" gegeben. Darauf aufbauend, werden die verschiedenen Perspektiven auf das Thema dargestellt. Abschließend werden die zentralen Formen der Bedrohung von Cyberkriminalität für Kommunen erklärt. Hierbei wird insbesondere auf Unterschiede und Überschneidungen eingegangen.

1.2 Begriffsklärung: Cyber und Sicherheit

Der Begriff „Cyber" hat mittlerweile breite Verwendung sowohl in der Wissenschaft, der Fachpraxis wie auch in der allgemeinen Bevölkerung und öffentlichen Diskussionen gefunden. Dennoch ist der Gegenstandsbereich, der mit *Cyber* gemeint ist, nicht eindeutig und v. a. nicht einheitlich definiert. Der Begriffsursprung ist abgeleitet aus dem Wort *Kybernetic*, welches wiederum auf dem griechischen Verb *kyvernó* beruht, was „steuern, lotsen oder herrschen" (*Rid*, 2016, S. 19) bedeutet, wobei *Thiedeke* auf das griechische Wort *kybernetike* verweist, was er mit „Kunst des Steuermanns" übersetzt (2004, S. 124). Geprägt wurde der Begriff von dem Mathematiker *Norbert Wiener* und seinem wirkmächtigen Buch „Kybernetik. Regelung und Nachrichtenübertragung im Lebewesen und in der Maschine" von 1948 (*Rid*, 2016, S. 19). Die Kybernetik versteht sich darin als Theorie der Maschinen, welche sich mit der Frage nach der Möglichkeit beschäftigt, dass Maschinen lernen, sich verhalten und denken können.

Dabei stellte eine wesentliche Entwicklungsdynamik der Zweite Weltkrieg dar, in welchem durch die massiven Luftangriffe der Deutschen, insbesondere auf England, die Kontrolle des Luftraums und die Möglichkeit der Luftabwehr zu einer zentralen Herausforderung wurden (*Rid*, 2016, S. 25-64). Das hauptsächliche Problem im Zusammenhang der Luftabwehr bestand darin, dass Flug- und Abwurfbahnen schlecht berechnet werden konnten. Die USA investierten viel Geld in wissenschaftliche Forschung in dem Bereich und auch Ingenieure trugen zu zentralen Entwicklungen bei, wodurch u. a. das Radar erfunden wurde. Einen weiterer Meilenstein der Kybernetik stellen die Arbeiten von *Ross Ashby* dar (*Rid*, 2016, S. 76 ff.), welche das Time-Magazin als die Erfindung der ersten „denkenden Maschine" (zitiert in ebd., S. 77.) bezeichnete. Kurz zusammengefasst bestand das Besondere an dem von *Ashby* entwickelten Gerät darin, dass die Maschine auf Außeneinwirkungen reagierte und selbstständig eine Lösung

3 Zum Beispiel zeigen *Nickerson/Varshney/Muntermann*, 2013, wie Taxonomien im Bereich Wirtschaftsinformatik regelgeleitet erstellt und validiert werden können.

fand, mit diesen umzugehen. Dies war für *Ashby* die zentrale Parallele zu dem menschlichen Gehirn, welches weniger dadurch gekennzeichnet sei, dass es **denkt**, als dass es **handelt**: *„Es erhält Informationen und unternimmt dann etwas aufgrund dieser Informationen"* (zitiert in *Rid*, 2016, S. 87). Dies beschreibt das Wesen der Kybernetik: Während es mechanische Maschinen bereits gab, beschäftigt sich die Kybernetik mit Maschinen, die sich verhalten und sich somit an menschlichen Denkprozessen orientieren, nur – so die Vorstellung, Hoffnung oder auch Befürchtung– besser und ohne menschliche Schwächen. 1963 bezeichnete die Mathematikerin *Alice Mary Hilton* die Neuerung der kybernetischen Idee als den Eintritt in ein Zeitalter der „Cyberkultur" (*Rid*, 2016, S. 133 ff.). Während die industrielle Revolution die körperlichen Fähigkeiten des Menschen erweiterten, welche von Maschinen effektiver ausgeführt werden konnten, erweiterten automatisierte, kybernetische Systeme die geistigen Fähigkeiten.

Heute fungiert die Entlehnung *Cyber* als Präfix zahlreicher Begriffe wie Cyber-Raum, Cyber-Krieg, Cyber-Sicherheit, Cyber-Sex und viele mehr. Wenn auch keine einheitliche Definition des Wortes auszumachen ist, so scheint dennoch die Voranstellung *Cyber* an einen Begriff dazu zu dienen, einen Bezug zu informationstechnischen Systemen, dem Internet und der Datenverarbeitung herzustellen. Ebenso trägt das vorliegende Handbuch den Begriff „Cyber" im Titel, verbunden mit dem Ziel, bei dem Leser eine Assoziation zu den vorgenannten Bereichen herzustellen.

In Bezug auf Kriminalität setzte sich der Begriff erst allmählich durch und löste damit u. a. die Begriffe „virtual criminology" oder Informations- und Kommunikationstechnik-Kriminalität, so genannte IuK-Kriminalität, ab, wobei letzteres teilweise immer noch innerhalb von Strafverfolgungsbehörden Anwendung findet (*Jaishankar*, 2007, S. 1; *Wernert*, 2014, S. 25 f.). Der Europarat erließ im Jahr 2009 die „Convention on Cybercrime", welche von Deutschland ratifziert wurde (*Wernert*, 2014, S. 25). Demnach gehören zu Cyberkriminalität Straftaten, die sich gegen Computerdaten und -systeme richten sowie solche, die mittels Computer, und somit auch u. a. mittels des Internets, begangen werden (ebd.). Hieraus folgt die Einteilung von Cyberkriminalität im weiteren sowie im engeren Sinn (siehe dazu weiter unten). Dem schloss sich auch ein Arbeitskreis der Innenministerkonferenz an und schlug vor, den bisherigen Begriff der IuK-Kriminalität durch Cybercrime, im folgenden Cyberkriminalität genannt, zu ersetzen (ebd., S. 26). Hierzu sollen Straftaten gehören, die sich gegen das *„Internet, weitere Datennetze, informationstechnische Systeme oder deren Daten richten"* (ebd.) bzw. auch strafrechtliche Handlungen, die durch Informationstechnik begangen werden, wie beispielsweise Cybermobbing. Insofern ist Cyberkriminalität nicht nur auf internetbezogene Straftaten fokussiert, indem auch Angriffe auf Daten und informationstechnische Systeme, unabhängig von einer Einbindung ins Internet, umfasst werden.[4]

Im Kontext von Cyberkriminalität ist ferner auch der Begriff „Sicherheit" von einer breiten und vielfältigen Verwendung geprägt. Im Allgemeinen beschreibt

4 Die verschiedenen Arten und Bedrohungsformen von Cyberkriminalität werden weiter unten erläutert.

der Begriff „Sicherheit" einen Zustand, der frei von Gefahr ist. Sicherheit wird im englischsprachigen Raum hingegen gleich durch vier Begriffe beschrieben: safety, security, protection und privacy (siehe u. a. *Klipper*, 2015). „Safety" entspricht der Betriebs- oder Funktionssicherheit, was bedeutet, dass das Objekt so funktioniert, wie es auch konstruiert wurde.

> *Negativbeispiel: Eine E-Mail-App für ein Smartphone wurde fehlerhaft programmiert und versendet jede E-Mail nicht nur an den Empfänger, sondern an das gesamte Kontaktverzeichnis. Hierbei ist die Anwendung fehlerhaft, ohne dass ein Dritter dies unbefugt von außen hervorruft.*

„Security" meint hingegen die Sicherung eines Systems gegen unerlaubten Zugriff, z. B. Veränderung oder Informationsgewinnung durch unautorisierte Dritte.

> *Negativbeispiel: Ein Hacker liest mithilfe einer Schadsoftware unverschlüsselte Passwörter aus einer Datenbank aus. Hierbei gelang es dem Täter, in das System einzudringen.*

„Protection" beschreibt die Datensicherheit oder auch Datensicherung[5], also den Schutz bestimmter Daten vor Verlust oder Zerstörung und nimmt dabei den technischen oder physischen Schutz des Datums selbst in den Vordergrund.

> *Negativbeispiel: Ein Hochwasser zerstört das Rechenzentrum eines Unternehmens, dessen Daten nicht durch ein weiteres, räumlich getrenntes Backup gesichert waren.*

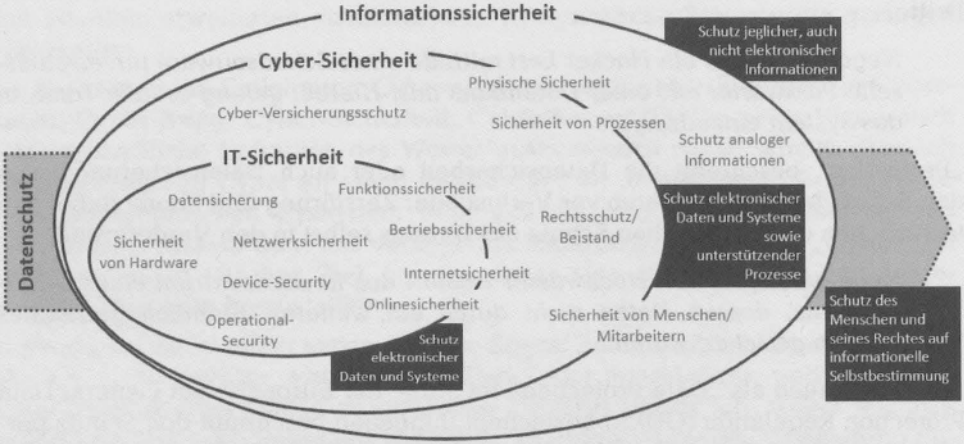
„Privacy", auch als „Data Protection" im Sinne der Europäischen General Data Protection Regulation (GDPR) bezeichnet, hingegen beschreibt den Schutz personenbezogener Daten, d. h. den Datenschutz, und somit das Recht jeder natürlichen Person auf informationelle Selbstbestimmung. Damit verlässt der Fokus beim Datenschutz vordergründig erst einmal die Technik und den Blick auf eine Organisation und ihre Systeme und wendet sich dem Menschen als Individuum zu. Es geht hier vorrangig um Verarbeitungen, also Prozesse und Systeme, die personenbezogene Daten, wie Kontaktdaten, Positionsdaten, Gesundheitsdaten, Informationen zu politischen Meinungen und sexueller Orientierung usw., speichern und nutzen sowie um die Frage, wie die natürliche Person diese Datennutzung überblicken und mitbestimmen kann. Die seit Mai 2018 wirksame Datenschutzgrundverordnung (DSGVO) regelt den Datenschutz europaweit und stellt darin auch gewisse Anforderungen an die Ausgestaltung von IT-Systemen und Prozessen und deren Sicherheit, was näher in den Kapitel 9 und 10 im vorliegenden Band dargestellt ist. Dadurch sind Datenschutz und Daten- bzw. Informationssicherheit eng miteinander verbunden, aber in ihrer Bedeutung keinesfalls gleichzusetzen.

---

5 Die ohnehin schwierige Abgrenzung der Begriffe wird zudem durch unterschiedliche Übersetzungen in das Englische verkompliziert. Die deutschen Begriffe „Datensicherheit" oder „Datensicherung" welche den physischen bzw. technischen Schutz von Daten selbst beschreiben sind beispielsweise nicht gleichzusetzen mit dem Begriff „Data Protection", welcher auf den rechtlichen Schutz von natürlichen Personen im Rahmen der Verarbeitung ihrer Daten abstellt.

Der in diesem Sinne verwandte Begriff der Sicherheit wird häufig um einen der Präfixe Informations-, IT- oder Cyber- ergänzt. In Fachkreisen des deutschsprachigen Raums wurde der Begriff IT-Sicherheit immer stärker durch den weiter gespannten Begriff der Informationssicherheit verdrängt, während in der öffentlichen Diskussion der Begriff Cybersicherheit stärker aus dem anglo-amerikanischen Raum übernommen wurde (siehe auch *Klipper*, 2015; Bundesamt für Sicherheit in der Informationstechnik, 2017). Auch wenn die Nutzung der Begriffe nicht immer einheitlich erfolgt, soll für diesen Beitrag die Begriffseinordnung gemäß der Abbildung 1 gelten.

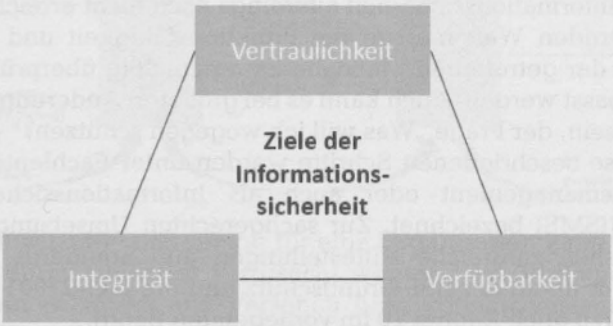
Abbildung 1: Einordnung verschiedener Sicherheitsbegriffe (Quelle: eigene Darstellung)



Unabhängig davon, welcher Begriff dem jeweiligen Nutzer näher liegt, verfolgen Informationssicherheit, Cybersicherheit und IT-Sicherheit ein gemeinsames Interesse: die Beschreibung der Schaffung von Resilienz gegen Gefahren aus dem Cyberraum. Gemeinhin wird diese Absicht durch die so genannten Ziele der Informationssicherheit *Vertraulichkeit*, *Integrität* und *Verfügbarkeit* dargestellt (siehe Abbildung 2). Informationssicherheit ist gegeben, wenn für ein bestimmtes System, einen Prozess oder eine Information die drei Schutzziele gewährleistet sind. Wenn die Vertraulichkeit eines Systems vorhanden ist, werden geschützte Informationen nicht unbefugt an Dritte preisgegeben. Nur berechtigte Personen können in zulässiger Weise auf die Informationen zugreifen (*Bundesamt für Sicherheit in der Informationstechnik*, 2017). Beispielsweise würde ein an einen Computer per USB angeschlossener Keylogger Benutzerzugänge und Passwörter, die über die Tastatur eingegeben werden, aufzeichnen und damit die Vertraulichkeit dieser Daten schädigen. Der Computer wäre aber weiterhin nutzbar und die Passwörter wären weiterhin korrekt und funktionsfähig. Das Schutzziel Integrität beschreibt die Einhaltung der Unversehrtheit bzw. Korrektheit, Vollständigkeit und Unverändertheit von Informationen sowie der Funktionsweise von Systemen (ebd.). Wenn beispielsweise ein Hacker durch einen Fernzugriff Einträge in einer Datenbank auf einem Computer verändert oder diese löscht, wäre die Integrität dieser Daten bzw. des Systems verletzt. Die

Verfügbarkeit von Systemen, Netzen und Informationen hingegen ist gewährleistet, wenn die Anwender diese wie vorgesehen nutzen können (ebd.). Ein Beispiel für die Verletzung des Schutzziels Verfügbarkeit ist eine Überlastung eines E-Mail-Servers durch massenhaft eingehende E-Mails (so genannter Denial-of-Service-Angriff, siehe unten). Durch die Überlastung der eingehenden E-Mails ist es dem Anwender nicht mehr möglich, selbst E-Mails zu lesen oder zu verschicken, da diese nicht mehr geladen werden können.

Abbildung 2: Ziele der Informationssicherheit (Quelle: eigene Darstellung)



Da der bereits genannte Sicherheitsbegriff „frei von Gefahr" in einer Welt mit beschränkten Ressourcen in der Realität nie erreicht werden kann, muss eine Organisation gezielte Maßnahmen und Strategien anwenden, um sich ausgehend von den eigenen Schutzzielen vor Gefahren zu schützen. Im Sinne eines bestmöglichen Schutzes vor dem Hintergrund von Wirtschaftlichkeits- und Praktikabilitätsaspekten sollte der Begriff „Sicherheit" als die Abwesenheit unvertretbarer Risiken verstanden werden. In diesem Satz stecken viele Fragen, die durch eine Organisation aufgenommen und angemessen beantwortet werden müssen. Was ist überhaupt ein Risiko? Welche Daten oder Prozesse sind der Organisation wichtig? Gegen was oder wen sollen sie geschützt werden? Wann ist ein Risiko vertretbar? Welche Schutzmaßnahmen sind wirkungsvoll? Welche Maßnahmen sind wirtschaftlich vertretbar?

Um diese Fragen zu beantworten, ist in einem ersten Schritt eine Analyse der eigenen Organisation nötig. Daran schließen sich in einem zweiten Schritt Überlegungen zu konkreten Schritten und Handlungen an, um die Informationssicherheit in der Organisation zu stärken, aber auch, auf welche Maßnahmen bewusst verzichtet wird und inwiefern dies vertretbar ist. Handlungen können beispielsweise in Form von Investitionen in technische Sicherheitsmaßnahmen – wie Antiviren-Software, Firewalls, Back-Up-Server oder Intrusion Detection Systeme – vorliegen. Oder eine Organisation entschließt sich, so genannte organisatorische Sicherheitsmaßnahmen – wie die Implementierung schriftlicher Sicherheitsrichtlinien, Freigabe- und Vertreterregelungen – oder die Erhöhung der Risikosensibilisierung von Mitarbeitern durch gezielte Schulungen und Trainings auszubauen (siehe hierzu auch Kapitel 12 im vorliegenden Band). Security by Design, also das Mitdenken von Sicherheit von vornherein und Security by Default, d. h. sicherheitsfreundliche Voreinstellungen von genutzten Verfah-

ren und Systemen, sind weitere Prinzipien, die Informationssicherheit unterstützen.

Für alle Sicherheitsmaßnahmen muss die Organisation zwischen den Faktoren Sicherheit, Kosten, Funktionalität und Komfort bzw. Praktikabilität mit Blick auf die vorab identifizierten Schutzziele abwägen. Als weitere große Herausforderung neben der Umsetzung einzelner Sicherheitsmaßnahmen gilt jedoch der Wandel einer Organisation zu einer gesunden Sicherheitskultur, der beispielsweise durch gutes Changemanagement begleitet werden kann.

Nach der Analyse und daraus abgeleiteter Umsetzung von Maßnahmen ist die angemessene Informationssicherheit allerdings noch nicht erreicht. In einer sich stetig verändernden Welt müssen die Funktionsfähigkeit und wirtschaftliche Sinnhaftigkeit der getroffenen Maßnahmen regelmäßig überprüft und gegebenenfalls angepasst werden. Auch kann es bei größeren Änderungen in der Organisation nötig sein, der Frage „Was will ich wogegen schützen?" erneut nachzugehen. All diese beschriebenen Schritte werden unter Fachleuten als Informationssicherheitsmanagement oder auch als Informationssicherheitsmanagementsysteme (ISMS) bezeichnet. Zur sachgerechten Umsetzung dieses Managements bestehen zahlreiche Hilfestellungen und Standards, von denen in Deutschland vor allem der BSI-Grundschutz und die ISO-27001 weit verbreitet sind (siehe hierzu auch Kapitel 10 im vorliegenden Band).

1.3 Perspektiven auf Cyberkriminalität

Wie eingangs beschrieben, ist der Bereich Cyberkriminalität dadurch gekennzeichnet, dass dieser aus sehr unterschiedlichen Perspektiven analysiert und diskutiert werden kann. Dies liegt u. a. an den zahlreichen verschiedenen Akteuren – wie Strafverfolgungsbehörden, IT-Dienstleister, Forscher, Täter, Opfer u. v. m. –, die das Phänomen aufgreifen. Die damit verbundenen unterschiedlichen Erkenntnisinteressen führen zu diversen Anknüpfungspunkten an das Thema, woraus sich unterschiedliche Begriffe und Begriffsverständnisse ergeben. Im Folgenden soll auf einige zentrale Perspektiven näher eingegangen werden. Dadurch soll dem Leser ein Einblick in die verschiedenen „Denkwelten" gegeben werden, die das Thema Cyberkriminalität zum Inhalt haben.[6]

1.3.1 Kausale Perspektive

Die kausale Perspektive stellt den logischen Ablauf eines Cyberangriffs dar. Dies geschieht zumeist auf höheren Aggregationsebenen, wobei die verschiedenen Elemente in vereinfachter Weise durch Ursache-Wirkungs-Beziehungen dargestellt werden. Es bestehen zahlreiche Klassifikations-Schemata, häufig Typologien, Taxonomien oder Frameworks genannt, die zum Ziel haben, Cyberangriffe zu systematisieren (*Agrafiotis et al.*, 2018; *European Union Agency For Network And Information Security*, 2016; *Howard/Longstaff*, 1998; *Jiang et al.*, 2013; *Jouini et al.*, 2014; *Simmons et al.*, 2014). Eine hochaggregierte Darstellung eines Cyberangriffs, die so genannte Informations-Risiko-Gleichung, liegt

6 Die beschriebenen Perspektiven stellen eine Auswahl der Autoren dar und erheben keinen Anspruch auf Exklusivität oder Vollständigkeit, sondern dienen lediglich der Einführung in das Thema.

beispielsweise der Information Risk Assessment Methodology (IRAM) des ISF zugrunde (*Information Security Forum*, 2017). Darin beschrieben werden die Begriffe Bedrohung, Sicherheitsevent und Vorfall, die häufig im Rahmen von Cyberangriffen, teilweise auch synonym, verwendet werden. Mithilfe dieser Begriffe lässt sich das Grundgerüst bilden, das jedem Cyberangriff zugrunde liegt (siehe Abbildung 3).

Abbildung 3: Logischer Ablauf eines Cyberangriffs (Quelle: eigene Darstellung)

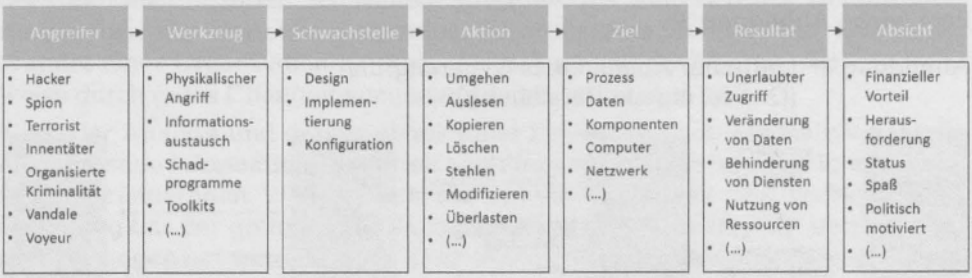
Eine vorerst schwebende Bedrohung für eine Organisation kann von außen her bestehen oder durch sie selbst verursacht werden. Das Vorhandensein dieser Bedrohung kann entweder aus Versehen bzw. zufällig zustande gekommen oder von den Tätern beabsichtigt worden sein. Wenn sich die Bedrohung realisiert, führt sie zu einem Sicherheitsevent. Das Sicherheitsevent wird im Optimalfall durch Kontrollen und Sicherheitsmaßnahmen gestoppt und bleibt vorerst ein Ereignis ohne weitere negative Folgen. Wenn das Event allerdings auf eine Schwachstelle trifft, die z. B. technischer oder organisatorischer Natur sein kann, spricht man von einem Vorfall. Dieser Vorfall kann wiederum Auswirkungen, wie z. B. Systemausfälle, Meldepflichten, finanzielle Kosten u. ä., nach sich ziehen. Dieser logische Ablauf kann auch anhand eines Beispiels dargestellt werden.

> *Beispiel: Ein frustrierter Mitarbeiter möchte seinem Arbeitgeber schaden. Diese potenzielle Bedrohung realisiert sich dadurch, dass die Webseite des Unternehmens durch massenhafte Aufrufe überlastet wird (Quelle: ein so genannter Denial of Service-Angriff, siehe unten). Je nachdem, ob der Angriff durch eine Sicherheitsmaßnahme, wie beispielsweise eine sachgerecht konfigurierte Firewall, verhindert werden konnte, bleibt das Ereignis ein Sicherheits-Event, das lediglich durch eine Meldung beim IT-Administrator auffällt. Da die Firewall an diesem Tag aber wegen Wartungsarbeiten nicht wie gewöhnlich funktioniert, wird die Attacke zu einem Sicherheitsvorfall. Durch die Überlastung der Webseite ist der Webshop des Unternehmens für einen Tag nicht erreichbar (das Schutzziel der Verfügbarkeit wurde beeinträchtigt), wodurch Umsatzeinbußen und Kosten für einen externen IT-Dienstleister entstehen sowie einige Kunden negativ über das Unternehmen berichten (Reputationsschäden).*

Nun ist es möglich, einen Vorfall auch einen Aggregationsgrad tiefer zu beschreiben. Dies taten beispielsweise *Howard* und *Longstaff* bereits im Jahre 1998 (vgl. Abbildung 4). Ohne im Folgenden weiter auf die einzelnen Inhalte

der Taxonomie einzugehen, stellen die Autoren einen Sicherheitsvorfall ebenfalls als Kausalkette dar, um einen Cyberangriff zu beschreiben.

Abbildung 4: Kausalkette eines Sicherheitsvorfalls
(Quelle: eigene Darstellung nach *Howard/Longstaff*, 1998)



Ein Angreifer nutzt mithilfe eines Werkzeugs eine Schwachstelle einer Organisation aus und führt dort eine Aktion gegen ein Ziel durch. Diese Aktion führt zu einem beabsichtigten oder nicht beabsichtigten Resultat, das der Angreifer mit einer bestimmten Absicht verfolgt hat. Zum Beispiel könnte ein Hacker ein Schadprogramm nutzen, um ein Firmennetzwerk mit schwach konfigurierter Firewall anzugreifen. Dort liest er beispielsweise Daten aus einem Computer aus und erhält dadurch Zugriff auf weitere Benutzerkennungen und Passwörter, deren digitale Identitäten der Hacker nun nutzen kann, um betrügerische Käufe durchzuführen.

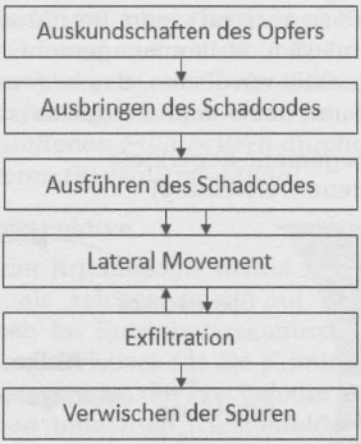
1.3.2 Forensische bzw. technische Perspektive

Forensische und technische Perspektiven auf Cyberangriffe stellen das tatsächliche und konkrete Vorgehen der Angreifer in den Fokus. Dabei geht es um detaillierte Handlungen und deren Auswirkungen auf Software, Hardware und Netze. In der Regel ist es das Ziel forensischer und technischer Analysen, den genauen Tathergang chronologisch bzw. phasenbasiert darzustellen, um zu verstehen, wie genau die Angreifer vorgegangen sind und welche Schwachstellen ausgenutzt wurden.

Cyberangriffe unterscheiden sich je nach Angreifer, deren Motivation und dem Ziel des Angriffs hinsichtlich ihrer Komplexität und dem Individualisierungsgrad (siehe auch Kapitel 2 im vorliegenden Band). Während einige Angreifer ungezielt versuchen, eine breite Masse an Opfern, z. B. durch Phishing-E-Mails und einfache Schadsoftware, zu erreichen, suchen sich andere Angreifer ihre Opfer etwas genauer (teilindividualisiert) oder dediziert sehr spezifisch aus (gezielter Angriff). Bei teilindividualisierten Angriffen investieren die Angreifer Vorbereitungszeit in einem gewissen Umfang, indem sie spezifische Opfergruppen, die bestimmte Merkmale aufweisen, anvisieren. Gezielte Angriffe sind nicht wahllos, sondern verfolgen ein konkretes Ziel gegenüber einem bestimmten Objekt. Die Angreifer verfügen über geeignete Ressourcen und bereiten den Angriff zum Teil sehr akribisch vor. Während die Angriffsphasen eines ungezielten Angriffs in der Regel relativ überschaubar sind, weisen gezielte Angriffe in idealisierter Form mehrere typische Angriffsphasen auf, die häufig

auch als Cyber-Kill-Chains (*Hutchins et al*, 2010) bezeichnet werden (vgl. Abbildung 5 nach *Steffens*, 2018).

Abbildung 5: Typische Angriffsphasen eines gezielten Angriffs (nach *Steffens*, 2018)



In der ersten Phase werden Informationen über das Opfer gesammelt und der Angriff vorbereitet. Dies kann beispielsweise durch technische Analysen wie Scans, durch das Auslesen öffentlicher Informationen (sog. Open Source Intelligence, kurz: OSINT) oder auch die Manipulation von Menschen (so genanntes Social Engineering, siehe unten) erfolgen. Anschließend wird der initiale Schadcode z. B. auf einem Computer im Zielnetzwerk installiert, wodurch er beispielsweise mittels einer versandten E-Mail oder durch ein eingeschleustes USB-Speichergerät gelangt. Das manuelle Ausführen des Schadcodes in der nächsten Phase ist nötig, da heutige Computer in der Regel keine unautorisierten Befehle entgegennehmen. So können beispielsweise die Benutzer durch gezielte Manipulation dazu gebracht werden, den Schadcode zu aktivieren. Nachdem der Schadcode ausgeführt wurde, können die Angreifer in der Regel auf den einen Computer im Zielnetzwerk zugreifen und diesen kontrollieren. Da sich beispielsweise die eigentlichen Zieldateien nicht auf diesem Computer befinden, wird das Lateral Movement (engl. für Seitwärtsbewegung) genutzt, um das Netzwerk auszukundschaften, sich dort auszubreiten und die Zieldateien zu identifizieren. Im Rahmen der Exfiltration müssen die Angreifer nun die Zieldateien in ihre eigene Hoheit überführen, z. B. per Upload oder E-Mail-Versand. Schließlich geht es in der letzten Phase darum, die Spuren des Angriffs beispielsweise durch das Löschen von Protokollierungsdateien und das Deinstallieren des verwendeten Schadcodes zu verwischen (nach *Steffens*, 2018).

1.3.3 Betriebswirtschaftliche Perspektive

Betriebswirtschaft hat auf den ersten Blick nicht viel mit Cyberkriminalität gemeinsam. Die Betriebswirtschaft hat zum Ziel, Organisationen durch aktive Steuerung in ihrer Zielerreichung zu unterstützen. Ziele einer Organisation können beispielsweise die Gewinnmaximierung für die Anteilseigner oder die Bereitstellung eines wichtigen Dienstes, wie der Wasserversorgung, für die

Bevölkerung sein. Diese Zielerreichung kann durch diverse Risiken beeinträchtigt werden. Spätestens seit der Digitalisierung wird in nahezu allen Bereichen der Gesellschaft Informationstechnik genutzt, um Produkte herzustellen oder Dienstleistungen anzubieten. Cyberkriminalität hat damit das Potenzial, diese Organisationsziele stark negativ zu beeinflussen und muss daher überwacht und gesteuert werden und wird so auch zu einem betriebswirtschaftlichen Themenfeld. Diese Tätigkeit nennt sich Risikomanagement. Aus betriebswirtschaftlicher Sicht ist Cyberkriminalität ein Risiko, das laufend identifiziert und analysiert, bewertet, behandelt und überwacht werden muss (vgl. Abbildung 6).

Abbildung 6: Risiko-Management-Regelkreis
(Quelle: eigene Darstellung)

Dieser so genannte Risiko-Management-Regelkreis muss einerseits Cyberrisiken in den unterliegenden Dimensionen eines Unternehmens identifizieren und bewerten, als auch Maßnahmen zur Verbesserung der Informationssicherheit in diesen Bereichen umsetzen und überwachen. Im Rahmen der Identifikation werden die Systeme und Prozesse einer Organisation systematisch nach möglichen Cyberrisiken durchleuchtet. In der anschließenden Analyse werden mögliche Auswirkungen der Risiken vor dem Hintergrund der eigenen Schutzziele untersucht. Als nächster Schritt werden die Risiken bewertet, wenn möglich sogar quantifiziert. Ein Risiko ist das Produkt aus seiner Eintrittswahrscheinlichkeit multipliziert mit dem potenziellen Schadensausmaß. Die so bewerteten Risiken werden nach einer Kosten-Nutzen-Abwägung behandelt. Risiken können so beispielsweise vermieden, vermindert, transferiert oder akzeptiert und getragen werden. Anschließend werden die Risiken dokumentiert und in einem Berichtswesen in angemessenen Intervallen den verantwortlichen Personen zur Verfügung gestellt. Ein Beispiel kann dieses Vorgehen etwas konkreter beschreiben.

> *Beispiel: Ein Wasserversorger hat neue digitale Pumpensysteme erhalten. Daher möchte die Geschäftsführung die neuen potenziellen Risiken für die Wasserversorgung bewerten und, sofern nötig, weitere Sicherheitsmaßnahmen ergreifen. In der Identifikations- und Analysephase fällt auf, dass die Pumpensysteme zwar technisch gemäß dem aktuellen Stand der Technik geschützt sind, jedoch die Mitarbeiter, die diese Anlagen bedienen, kaum für das Thema Informationssicherheit sensibilisiert sind. Daher besteht die Gefahr, dass Angreifer z. B. mithilfe einer Phishing-Attacke (siehe unten) die Systemzugänge der Mitarbeiter erlangen und missbrauchen und*

die bisher implementierten Sicherheitsmaßnahmen umgehen. Die Risikobewertung ergibt, dass die Wahrscheinlichkeit für eingehende Phishing-E-Mails relativ hoch und ein Ausfall der Wasserversorgung verheerende Folgen hätte. Die Behandlung des Risikos erfolgt auf drei Ebenen. Zum einen werden die Firewall-Regeln verschärft, um potenzielle Phishing-E-Mails von vornherein abzublocken (Risikovermeidung). Zum anderen werden eine Arbeitsanweisung und ein Notfallplan entworfen, wie im Falle eines Angriffs zu verfahren ist, um potenzielle Auswirkungen gering zu halten (Risikoverminderung). Zudem wird ein so genanntes Awareness-Training mit den betroffenen Mitarbeitern durchgeführt, um sie für Cyberrisiken zu sensibilisieren (Risikovermeidung).

1.3.4 Kriminologische Perspektive

Das Erkenntnisinteresse der Kriminologie richtet sich auf die Beschreibung des Phänomens Kriminalität als solches sowie auf die Frage nach Ursachen-Wirkungszusammenhängen im Entstehungskontext von und im Umgang mit strafbaren Verhalten. Charakteristisch für die Kriminologie ist eine breite Interdisziplinarität, wobei die Soziologie, die Psychologie und die Rechtswissenschaft die stärksten Bezüge zu den genannten Themenfelder aufweisen. Hierbei ist die Kriminologie jedoch von der Kriminalistik abzugrenzen. Letztere fokussiert auf Methoden und Herangehensweisen, um bestimmte Straftaten aufzuklären im Sinne einer erfolgreichen polizeilichen Ermittlung. Die Kriminalistik ist somit eher die Wissenschaft der Beweisfindung und -sicherung, mit dem Ziel, einen Täter zu identifizieren. Die Kriminologie hingegen nimmt eine verstärkt soziologische Perspektive auf Kriminalität ein, begreift dieses als soziales Phänomen und stellt die Frage danach, warum dieses in einem weiteren Sinn überhaupt entsteht und sich entwickelt (und weniger, wie es zu einer einzelnen Tat kommt). Ferner umfasst sie auch die Analyse der Reaktionen auf Straftaten, d. h. der Strafformen, und dessen Wirkung bezüglich erneuter Kriminalitätsentstehung.

Vor diesem Hintergrund richtet sich die kriminologische Perspektive in Bezug auf Cyberkriminalität zunächst auf das Ausmaß und die Entwicklung vielfältiger Erscheinungsformen von Straftaten, die in Verbindung mit der Internet- und Computernutzung stehen. Insofern stellt dies einerseits eine deskriptive Betrachtungsweise dar, bei welcher Fragen danach, wer (Privatnutzer, Unternehmen, Behörden sowie weitere Merkmale wie Alter, Geschlecht, Nutzungsverhalten usw.) wie häufig und welche Arten von Cyberkriminalität erlebt werden, nachgegangen wird. Ferner gehört zum kriminologischen Untersuchungsgegenstand jedoch auch die Frage nach den Tätern (*Huber*, 2019, S. 31-61; S. 149-162) sowie dem Handeln der Strafverfolgungsbehörden (*Stiller et al.*, 2020). Des Weiteren gehört zur Cyberkriminalität die Untersuchung von Einflussfaktoren auf die Erhöhung des Risikos, Opfer von Straftaten mit einem Bezug zum Internet bzw. zu informationstechnische Systeme zu werden.

Interessanterweise stellt sich die oben skizzierte Abgrenzung von Kriminologie und Kriminalistik ebenso in Bezug auf Cyberkriminalität. So hat der Herausgeber der Fachzeitschrift *International Journal of Cyber Criminology*, *Jaishankar* (2007), im Editorial der ersten Ausgabe die Notwendigkeit gesehen, *cyber criminology* als eigenständige Disziplin herauszustellen und von *cyber forensics*

zu unterscheiden: *„There is a need to identify the differences between cyber criminology and cyber-forensics. Cyber-forensics deals exclusively with the investigation of cyber crimes, whereas cyber criminology deals with the causation of cyber crimes"* (S. 1). Rund zehn Jahre später formiert sich auch in Deutschland eine *scientific community* zu dem Themenbereich Cyberkriminologie (*Rüdiger/Bayerl*, 2020). Hinsichtlich der Vielfalt der Bedrohungsformen von Cyberkriminalität (mehr dazu siehe unten) lässt sich jedoch ein Schwerpunkt der Untersuchungen auf Deliktsbereiche erkennen, die auch aus dem analogen Raum bekannt sind und sich inzwischen fest im digitalen Kontext etabliert haben, wie beispielsweise Cybermobbing (*Bergmann/Baier*, 2018; *Bergmann et al.*, 2019). Kriminologische Untersuchungen zu Straftaten, die sich gegen informationstechnische Systeme, d. h. Daten und Computer sowie den damit verbundenen Anwendungen, richten, liegen bisher jedoch wenig im deutschsprachigen Raum vor (*Bergmann et al.*, 2018; *Dreißigacker et al.*, 2020).

1.3.5 Perspektive der Strafverfolgung

Zur Kategorisierung der Vielzahl unterschiedlicher Cyberkriminalitätsformen stützt sich die Strafverfolgung auf eine Einordnung in zwei Bereiche: Cyberkriminalität im weiteren und Cyberkriminalität im engeren Sinn (*Bundeskriminalamt*, 2019). Diese Unterscheidung, welche im Jahr 2000 im Rahmen eines UN-Kongresses eingeführt wurde, ist mittlerweile auch im internationalen Kontext weit verbreitet (ebd.).

Der Bereich Cyberkriminalität im weiteren Sinn umfasst Straftaten, die mittels Informations- und Kommunikationstechnik durchgeführt werden, auf diese selbst jedoch nicht abzielen (*Bundeskriminalamt*, 2019). Hierzu gehören beispielsweise Phänomene wie Cybermobbing und -stalking, aber auch Erpressungshandlungen oder Betrugsdelikte wie der Warenbetrug. Die Tathandlungen finden mittels Internetplattformen bzw. E-Mails und dergleichen statt, allerdings wird die IT-Technik selbst nicht angegriffen, wie es beispielsweise eine Schadsoftware bewirkt. Das Internet bzw. Informationssysteme sind insofern eher das Tatmittel als das Tatobjekt.

In Bezug auf den Bereich Cyberkriminalität im engeren Sinn verhält sich dies anders. Hierzu gehören Straftaten, „die sich gegen das Internet, weitere Datennetze, informationstechnische Systeme oder deren Daten richten" (*Bundeskriminalamt*, 2019). Insofern ist das Internet bzw. informationstechnische Systeme hier nicht nur Tatmittel, sondern werden direkt von der Straftat angegriffen, wie beispielweise durch ein Schadprogramm, das Daten zerstört, oder das Eindringen in ein System, um Daten und Nutzeraktivitäten auszuspähen.

Während Cyberkriminalität im weiteren Sinn strafrechtlich den zugrundeliegenden Delikten einfach zugeordnet werden kann, gestaltet sich dies in Bezug auf Cyberkriminalität im engeren Sinn schwieriger. Das *Bundeskriminalamt* trifft hierbei folgende Einordnung (2019):

Computerbetrug als Cyberkriminalität im engeren Sinn (§ 263a StGB): Hierbei „betrügt" der Täter quasi ein Computersystem, indem er beispielsweise Kredit- oder EC-Karten nutzt, die er rechtswidrig erlangt hat und sich dem Computer gegenüber als jemand anderes ausgibt, als er ist. Hierunter fallen aber auch

andere Formen des Einwirkens auf einen Datenverarbeitungsvorgang, um sich oder andere Vermögensvorteile zu verschaffen.

Sonstiger Computerbetrug (§ 263a Abs. 1 und 2 StGB sowie Vorbereitungshandlungen gemäß § 263a Abs. 3 StGB): Weitere Betrugsformen, wie beispielsweise das Herstellen von Programmen, um einen Computerbetrug durchführen zu können.

Ausspähen und Abfangen von Daten, inklusive Vorbereitungshandlungen und Daten-Hehlerei (§§ 202a, 202b, 202c, 202d StGB): Dies umfasst den Diebstahl von identitätsbezogenen Daten, wie beispielsweise Konto- und Kreditkartendaten bzw. den Verkauf solcher Daten.

Fälschung beweiserheblicher Daten bzw. Täuschung im Rechtsverkehr (§§ 269, 280 StGB): Beispiele hierfür sind E-Mails, welche einen scheinbar bekannten Absender vortäuschen wie der Name einer Bank, um den Empfänger der E-Mail zu täuschen und ihn zur Herausgabe von Kontodaten und dergleichen zu bewegen.

Datenveränderung bzw. Computersabotage (§§ 303a, 303b StGB): Hierunter fallen Tathandlungen, die Daten beschädigen bzw. verändern oder verschlüsseln, sodass der Nutzer auf diese nicht mehr zugreifen kann. Ausgelöst wird dies beispielsweise durch eine Schadsoftware (siehe unten) wie einen Wurm oder ein Computervirus.

Missbräuchliche Nutzung von Telekommunikationsdiensten (§ 263a StGB): Dies ist eine Sonderform des Computerbetrugs, bei der der Täter sich beispielsweise in ein Wireless Local Area Network (WLAN) einwählt und somit unberechtigt über einen fremden Anschluss kostenpflichtige Telekommunikationsdienste nutzt, z. B. Auslandstelefonate.

Nicht alle Formen von Bedrohungen gegen Informationssysteme lassen sich eindeutig einem der beiden Bereiche von Cyberkriminalität im engeren und weiteren Sinn zuordnen. So adressiert beispielsweise das Phänomen des Ransomware-Angriffs, welches weiter unten erläutert wird, beide Formen: Im Kontext von Ransomware werden in einem ersten Schritt Daten verschlüsselt, sodass der Nutzer auf diese nicht mehr zugreifen kann (Cyberkriminalität im engeren Sinn), um daraufhin ein Lösegeld für die Datenentschlüsselung zu fordern (d. h., eine Erpressungshandlung und somit Cyberkriminalität im weiteren Sinn).

Ferner weist das aufgegriffene Beispiel eines Ransomware-Angriffs jedoch auch noch auf eine weitere Problematik der Perspektive der Strafverfolgung bzw. der rechtlichen Einordnung hin. Die Tat eines Ransomware-Angriffs, also die Verschlüsselung von Daten, auf welche sich anschließend eine Erpressungshandlung bezieht, treffen juristisch eingeordnet zwei Deliktsbereiche: Datenveränderung bzw. Computersabotage gemäß §§ 303a, 303b StGB und Erpressung gemäß § 253 StGB. Somit beschreiben die strafrechtlichen Normen des Strafgesetzbuchs nicht die Bedrohungsform Ransomware als Ganzes, d. h. in seiner besonderen Form der Kopplung von zwei Handlungen. Vielmehr geht ein Teil des Ransomware-Angriffs in einer althergebrachten StGB-Norm auf, ein weiterer wird einer neueren StGB-Norm zugeordnet, wobei letztere zumindest den Bezug zu Cyberkriminalität erkennen lässt.

Juristisch mag dies kein Problem darstellen, es zeigt sich keine Strafbarkeitslücke oder dergleichen. Vielmehr können teilweise Delikte bzw. strafbare Handlungen mit einem Cyberbezug gängigen Strafrechtsnormen zugeordnet werden, welche auch Handlungen aus der so genannten analogen Welt aufnehmen wie beispielsweise die eben erwähnte Erpressung. Zur Beschreibung der Bedrohungsformen von Cyberkriminalität, welche in dem vorliegenden Beitrag erfolgen soll, scheint die juristische Einordnung jedoch wenig geeignet zu sein, da der Cyberkontext nicht immer klar erkennbar ist. Dies dürfte sicher auch ein Grund dafür sein, dass im Bereich von Cyberkriminalität eine Vielzahl von Wortbildungen und -neuschöpfungen vorzufinden ist, da die Strafrechtsnormen das Phänomen nicht angemessen abbilden. Dies unterscheidet Cyberkriminalität elementar von anderen Kriminalitätsbereichen, wie beispielsweise Gewalt- oder Eigentumsdelikten, bei welchen eine Orientierung an den Definitionen im Sinn des Strafgesetzbuchs auch außerhalb von juristischen Betrachtungsweisen Anwendung findet.

1.4 Formen der Bedrohung von Cyberkriminalität

Die verschiedenen Perspektiven, die bezüglich des Phänomenbereichs Cyberkriminalität eingenommen werden können, führen, wie mehrfach angesprochen, zu verschiedenen Darstellungsformen, abhängig vom jeweiligen Erkenntnisinteresse. Um dennoch darzustellen, welche Tathandlungen und Angriffsformen unter Cyberkriminalität, insbesondere auch im vorliegenden Handbuch, verstanden werden, werden im folgenden Abschnitt zentrale Formen der Bedrohung beschrieben und dahingehend erläutert, inwiefern diese sich voneinander abgrenzen bzw. auch überschneiden. Dabei wird jedoch nur auf solche Bedrohungsformen eingegangen, die eine Gefahr für Behörden darstellen. Nicht erwähnt werden dadurch beispielsweise der Bereich des Cybermobbings, Cyberstalkings und die Verbreitung verbotener Inhalte wie im Kontext von kinderpornographischen Darstellungen. Weiter beschränkt sich dieser Abschnitt auf die Beschreibung des Phänomens. Die Ausmaße der Angriffe, d. h. wie oft diese in Deutschland vorkommen und wer davon betroffen ist, sind hingegen Thema des Kapitels 3 im vorliegenden Band.

1.4.1 Schadsoftware-Angriff

Beispiel: Der Erhalt einer E-Mail mit dem Betreff „Bewerbung als Justizfachangestellter" war nichts Ungewöhnliches für die Behörden der Hessischen Justiz. Im beigefügten Anhang vermuteten die Behördenmitarbeiter ein Anschreiben, einen Lebenslauf und weitere typische Bewerbungsunterlagen. Tatsächlich handelte es sich bei der massenhaft versandten E-Mail jedoch nicht um eine Initiativbewerbung, sondern um einen Cyberangriff.[7] *Der Anhang beinhaltete über eine Schadsoftware in Form eines Virus, welche durch Öffnen der beigefügten Datei in das Computersystem gelangte. Betroffen waren davon u. a. zwei Amtsgerichte, die in der Folge nicht mehr auf eigene Daten zugreifen konnten. Durch die vorherige Datensicherung*

7 https://info-pb-hmdj.hessen.de/pressearchiv/pressemitteilung/gefaelschte-e-mails-mit-verschluesselungs-trojanern-als-bewerbungen-getarnt (aufgerufen am 4.1.2020).

konnten diese jedoch wiederhergestellt werden. Auch in jüngerer Zeit waren Behörden immer wieder von Schadsoftware betroffen, so wie das Berliner Kammergericht[8]. Anders als bei den Initiativbewerbungen erschienen in der Absenderzeile jedoch bekannte Namen von Personen, mit denen der Empfänger kürzlich E-Mail-Kontakt hatte. Auch die Signatur war vergleichbar. Im Anhang befand sich wiederum eine Schadsoftware.

Großen Schaden richtete zum Beispiel auch der Wurm Stuxnet an, von dem insbesondere industrielle Fertigungsanlagen betroffen waren, die Programme von Siemens nutzten, wie beispielsweise Anlagen zur Urananreicherung im Iran.[9] Der Wurm gelangte über einen USB-Stick in die betroffenen Systeme und verbreitete sich selbstständig weiter. Hierbei gelangte er auch auf Computer, die nicht in einem lokalen Netzwerk oder mit dem Internet verbunden waren.

Beispiele von Schadsoftware lassen sich zahlreich finden. Dies liegt u. a. auch daran, dass sie oft verbunden sind mit weiteren Tathandlungen, wie beispielsweise Erpressungen. Schadsoftware hat dabei auch schon große Unternehmen wie die Deutsche Bahn oder Maersk[10] aber auch Unternehmen der öffentlichen Daseinsvorsorge wie das Lukas-Krankenhaus (Dahmen/Krämer, 2018) in Neuss getroffen. Während in den zuerst genannten zwei Beispielen die gesicherten Backup-Dateien den Betriebsablauf schnell wieder herstellen konnten, führt in vielen anderen Fällen der verhinderte Zugang bzw. der Ausfall eigener IT-Systeme zu enormen Betriebsunterbrechungen und Kosten.

Schadsoftware (engl.: *malware*) bezeichnet eine Software, die sich schädigend auf ein Computersystem auswirkt (siehe u. a. *Huber*, 2019, S. 75-98; *Wernert*, 2014, S. 143 f.). In der Folge ist der Zugriff auf Daten nicht mehr möglich oder Programme und Anwendungen können nicht mehr genutzt werden. Dabei handelt es sich jedoch bei dem Begriff Schadsoftware um eine Sammelbezeichnung von sehr unterschiedlichen Formen von Software und Schädigungen. Zu den bekanntesten Arten in diesem Kontext zählen sicherlich Viren, Würmer und Trojaner, wobei es noch viele weitere Bezeichnungen und Unterarten gibt. Während ein Virus, vereinfacht gesagt, an einem Programm oder einer Datei haftet und nur mittels dieser übertragen werden kann, verfügt ein Wurm über die Fähigkeit, sich selbstständig zu verbreiten bzw. zu vervielfältigen, z. B. indem Kontaktdaten aus digitalen Adressbüchern und E-Mailprogrammen oder Netzwerkverbindungen genutzt werden. Demnach kann bei einem Wurm für die weitere Verbreitung im Netzwerk genügen, wenn beispielsweise ein Mitarbeiter einer Behörde einen infizierten E-Mail-Anhang öffnet. Ein Trojaner wiederum kann sowohl einen Wurm als auch einen Virus enthalten; kennzeich-

8 https://www.lto.de/recht/justiz/j/kg-berlin-Cyberangriff-trojaner-virus-offline/ (aufgerufen am 4.1.2020).

9 https://www.kaspersky.de/blog/five-most-notorious-cyberattacks/18055/ (aufgerufen am 5.1.2020).

10 https://www.spiegel.de/netzwelt/netzpolitik/moller-m-rsk-cyberangriff-kostet-reederei-hunderte-millionen-a-1163111.html (aufgerufen am 13.2.2020).

nend hierbei ist, dass das Schadprogramm über eine scheinbare harmlose Anwendung quasi versteckt auf das Computersystem gelangt. Ein Trojaner kann somit in Form eines E-Mail-Anhangs oder als Zip-Datei gegeben sein, welche eine gewöhnliche Kommunikation suggeriert (z. B. das Erhalten einer Rechnung), in der angehängten Datei jedoch eine schädigende Software enthalten ist (siehe u. a. *Büchel/Hirsch*, 2014, S. 86 f.).

Ebenso wie die Arten von Schadsoftware sind die Wege der Infizierung eines Computersystems mit Schadsoftware vielfältig. Diese kann beispielsweise durch das eben schon erwähnte Öffnen von E-Mail-Anhängen oder das Anschließen von Datenträgern (z. B. USB-Sticks) erfolgen. Ferner kann sich Schadsoftware auch ausschließlich durch das Aufrufen entsprechend programmierter Internetseiten verbreiten (so genannter „Drive-by-Download", *Wernert*, 2014 oder auch „Drive-by-Infection", *Büchel/Hirsch*, 2014, S. 29), welche der Internetnutzer beispielsweise deshalb öffnet, weil er einer entsprechenden Aufforderung in einer fingierten E-Mail nachkommt. Ebenso kann sich Schadsoftware auch in Video- oder Sounddateien, welche online angeboten werden, befinden (*Bundeskriminalamt*, 2019, S. 28).

Schadprogramme nutzen Schwachstellen und Sicherheitslücken in Systemen aus, so genannte *Exploits* (von engl. to exploit, dt.: ausnutzen). Diese können, wie im unten näher ausgeführten Beispiel zu dem Vorfall *WannaCry*, auch durch veraltete Betriebssysteme, für die keine Sicherheitsupdates mehr zur Verfügung gestellt werden, bestehen. Insofern ist neben dem Vorhandensein von Virenscannern und dergleichen auch das Verwenden aktueller Software eine wichtige Schutzmaßnahme. Erkennen Hersteller Sicherheitslücken in ihren Programmen, stellen sie gewöhnlich eine Art Update bereit, mittels welchem diese Lücken geschlossen werden kann, so genannte *Patches* (dt.: Flicken/Pflaster). Demgemäß gehört ferner zur Prävention von Schadsoftware-Angriffen, dass aktuelle Sicherheitspatches, die von den Herstellern zur Verfügung gestellt werden, von den Nutzern zeitnah registriert und installiert werden (siehe auch Kapitel 11 im vorliegenden Band).

Nicht immer bemerkt der Nutzer vorhandene Schadsoftware, da einige Programme weniger darauf abzielen, Daten zu manipulieren oder zu verschlüsseln, sondern darauf, einen illegalen Zugang zu Daten zu verschaffen (siehe hierzu auch die Ausführungen zu Spyware weiter unten). Gemeinsam ist den Arten von Schadsoftware, dass sie sich schädigend auf die Funktionsfähigkeit des Computersystems auswirken bzw. Unbefugten Zugang zu Daten verschaffen. Schadsoftware wird nicht ausschließlich zur Schädigung von Dateien und Programmen eingesetzt, vielmehr ist sie oftmals Bestandteil verschiedener weiterer Bedrohungsformen wie beispielsweise Botnetze, Ransomware, Spyware und Phishing.

1.4.2 Botnetz

Beispiel: Ein internationales Team verschiedener Strafverfolgungsbehörden hat das so genannte Botnetz „Avalanche" (dt.: Lawine) ausgehoben.[11]

11 https://www.bsi-fuer-buerger.de/BSIFB/DE/Risiken/BotNetze/Avalanche/botnetz_ava lanche_node.html (aufgerufen am 4.1.2020).

Dabei handelte es sich um einen Zusammenschluss zahlreicher Computer mit dem Ziel, eine hohe Rechnerleistung mehrerer Server zu erzielen. Allein in Deutschland waren mehr als 50000 Rechner Teil dieses Botnetzes, an welchem die Täter seit sieben Jahren arbeiteten.[12] *Die Inhaber dieser Rechner waren jedoch keine Täter, vielmehr wurden sie durch ein Schadprogramm ohne ihr Wissen Teil des Botnetzes. Gemerkt haben sie dies in ihrem normalen Gebrauch des Computers nicht, lediglich die für ihre Anwendungen verfügbare Rechnerleistung dürfte etwas eingeschränkt und der Stromverbrauch höher gewesen sein. Das Botnetz Avalanche wurde zum Versenden großer Mengen an Phishing- und Virenmails genutzt. Die festgenommenen Täter haben jedoch vor allem Geld insofern damit erwirtschaftet, dass sie das Botnetz aufgebaut und zur Verfügung gestellt haben, sodass andere sich in dieses „einkaufen" konnten, um es für weitere Angriffe zu nutzen. So wurde beispielsweise das Nutzen des Botnetzes „Mirai" (japanisch, dt.: Zukunft) im Internet für rund 7500 Dollar angeboten.*[13]

Angelehnt an das englische Wort *robot* (dt.: Roboter) bezeichnen Bots weitestgehend eigenständig arbeitende Computerprogramme (siehe u. a. *Wernert*, 2014, S. 143-145), d. h., eine Software, „[...] *die entweder automatisch oder unter minimaler menschlicher Einwirkung Befehle ausführt, auf Nachrichten antworten oder Routineaufgaben durchführt*" (*Harringer*, 2018, S. 259). Bots kommen nicht nur für strafbare Handlungen zur Anwendung. Legale Bots liegen beispielsweise Chatfunktionen im Zusammenhang mit Kundenservice-Portalen zugrunde. Auf Internetseiten großer Online-Händler können hierbei Kunden ihr Anliegen schriftlich in einer Eingabemaske darlegen und erhalten Antworten bzw. weiterführende Informationen. Dabei treten die Kunden in eine quasi automatisierte Kommunikation, denn auf der anderen Seite befindet sich nicht ein Mitarbeiter des Unternehmens, vielmehr vermag es das Programm, d. h. der Bot, selbstständig auf die geschilderten Probleme zu antworten. Weiter werden legale Botnetze auch für wissenschaftliche Forschung genutzt, um mittels erhöhter Rechenleistung zum Beispiel aufwendige Datenanalysen vornehmen zu können (*Harringer*, 2018, S. 262).

Nicht legal ist die Verwendung von Bots beispielsweise im Bereich des systematisierten Abfangens von E-Mail-Adressen, um diese dann u. a. für Werbemaßnahmen und ähnliches zu verkaufen (*Wernert*, 2014, S. 143). Um Zugang zu Computersystemen und somit Daten zu erlangen, wird wiederum eine Schadsoftware eingesetzt.

Der Einsatz von Schadsoftware ist auch der erste Schritt bei der Erstellung von Botnetzen, wobei die Infizierung des Computers mit der Software auf den vielfältigen Wegen, wie oben beschrieben, stattfinden kann. In einem zweiten Schritt wird durch die Schadsoftware bei der Erstellung eines Botnetzes jedoch nicht eine Veränderung oder Beeinträchtigung der Datennutzung erwirkt, sondern eine Verbindung zu einem speziellen Server hergestellt. Massenhaft

12 https://www.heise.de/newsticker/meldung/Malware-Attacken-ueber-Avalanche-Botnet-Drahtzieher-vor-Gericht-4423942.html (abgerufen am 4.1.2020).

13 https://www.zeit.de/digital/internet/2016-10/ddos-attacke-dyn-internet-der-dinge-us-wahl (aufgerufen am 4.1.2020).

durchgeführt, ist dieser zentrale Server mit vielen Computersysteme verbunden, ohne die Zustimmung oder das Wissen der Inhaber der Computer. Durch dieses Vorgehen wird die Rechenleistung von einer Vielzahl von Computern gebündelt zu einem *Netz*, einem so genannten *Botnetz*. Die jeweiligen Inhaber der Computer bemerken oftmals nicht, dass sie Teil eines Botnetzes sind. Dies liegt daran, dass die Daten und sonstige Anwendungen wie gewohnt verfügbar sind, lediglich die Rechnerleistung ist beeinträchtigt, was sich in einer geringeren Geschwindigkeit bei der Ausführung der Programme sowie einem erhöhten Stromverbrauch bemerkbar machen könnte.

Das Erzielen einer hohen Rechenleistung durch Botnetze kann ebenso wie Schadsoftware für sehr unterschiedliche weitere Straftaten genutzt werden. Durch Botnetze können beispielsweise Spam-Mails massenhaft verschickt, digitale Währung erstellt (so genanntes *Krypto-Mining*) oder (D)Dos-Angriffe (Näheres dazu siehe unten) durchgeführt werden (*Bundeskriminalamt*, 2019, S. 28-30). Um ein Botnetz für illegale Zwecke zu nutzen, muss sich ein potenzieller Täter dieses nicht unbedingt selbst erstellen. Der Zugang zu einem Botnetz kann auch käuflich erworben werden, was auch als *crime-as-a-service* benannt wird.

1.4.3 Ransomware

Beispiel: Der weltweit größte Ransomware-Angriff von dem mehr als 200000 Computer in 150 Ländern betroffen waren, begann im Mai 2017 an einem Freitag.[14] *Binnen kürzester Zeit verbreitete sich hierbei vor allem in Europa und den USA eine Schadsoftware, die die Daten des jeweiligen Computersystems verschlüsselte. Die rasante Verbreitung wurde dadurch begünstigt, dass es sich bei der Schadsoftware um einen Wurm handelte. War dieser erstmal durch Anklicken eines Anhangs oder dergleichen auf einen Computer gelangt, breitete er sich selbstständig im Netzwerk aus und ging so auf andere Computer über. Dabei wurde eine Schwachstelle von veralteten Versionen von Windows ausgenutzt, die Microsoft bekannt war und die in neueren Windows-Versionen geschlossen werden konnte.*

WannaCry führte zu einer Verschlüsselung der Daten, d. h., der Nutzer konnte nicht mehr auf seine Benutzeroberfläche, Ordner und demnach auch Daten zugreifen. Der Bildschirm zeigte den Angriff an (siehe Abbildung 7) und forderte zu einer Geldzahlung in Höhe von 300-600 US-Dollar auf, welche in Form von Bitcoins zu erbringen sein sollten. Erfolgt diese Lösegeldzahlung, so die Botschaft, würden die Daten wieder frei gegeben werden.

Betroffen waren Privatnutzer, Behörden und Unternehmen, davon u. a. die Deutsche Bahn, die keinen Zugriff auf ihre Anzeigetafeln mehr hatte. Großbritannien verzeichnete schwere Folgen aufgrund des Angriffs, hierunter vor allem das Nationale Gesundheitszentrum: Krankenhäuser waren

14 https://www.spiegel.de/netzwelt/web/wannacry-attacke-fakten-zum-globalen-Cyber angriff-a-1147523.html (aufgerufen am 4.1.2020); https://www.kaspersky.de/blog/five-most-notorious-cyberattacks/18055/ (aufgerufen am 4.1.2020).

stark beeinträchtigt in ihrer Arbeit, medizinische Geräte konnten teilweise nicht mehr genutzt werden, was dazu führte, dass Patienten abgewiesen bzw. nach Hause geschickt wurden.[15]

Abbildung 7: Bildschirmdarstellung des Ransomware-Angriffs *WannaCry*[16].

Nicht immer ist bei einem Ransomware-Angriff der Erpressungsversuch offensichtlich. Im Fall des so genannten BKA-Trojaners wird dem Betroffenen z. B. suggeriert, eine Nachricht vom Bundeskriminalamt zu erhalten (Büchel/Hirsch, 2014, S. 86 ff.). Diese enthält die Information, dass der Nutzer verbotene Seiten aufgerufen habe, die Daten deshalb verschlüsselt wurden und eine Strafzahlung zu entrichten sei. Variationen hiervon rufen zu dem Anruf einer kostenpflichten Rufnummer auf oder dem Erwerb eines vermeintlichen Programms zu Wiederherstellung der Daten.

Bei einem so genannten Ransomware-Angriff gelangt zunächst eine Schadsoftware auf das Computersystem (siehe u. a. *Büchel/Hirsch*, 2014, S. 84-101). Dieses führt dazu, dass Daten verschlüsselt, manipuliert oder anderweitig beschädigt werden. Der Nutzer kann in der Folge seine Daten nicht nutzen. Dabei

15 https://www.heise.de/newsticker/meldung/WannaCry-Was-wir-bisher-ueber-die-Ransomware-Attacke-wissen-3713502.html (aufgerufen am 4.1.2020).

16 Bildquelle: https: // techsupportexpert.com / wannacry - ransomware - spreads - aggressively - across - networks - holds - files - ransom / ransom - demand - screen - displayed - by - wannacry-trojan/.

wird er in einem zweiten Schritt aufgefordert, eine Art Lösegeld zu bezahlen, um wieder den Zugang zu den Daten zu erlangen. Insofern ist ein Ransomware-Angriff eine Kombination aus Schadsoft*ware* und Lösegelderpressung (engl.: ransom, dt.: Lösegeld).[17]

Im klassischen Fall fährt der Nutzer seinen PC hoch. Statt die gewohnte Anwenderoberfläche, beispielsweise den so genannten Desktop, zu sehen, erscheint nun jedoch ein Schreiben des Täters auf dem Bildschirm (siehe Abbildung 7). Hierbei wird der Nutzer darüber informiert, dass die Daten verschlüsselt wurden und somit kein Zugang mehr möglich sei. Um wieder an die Daten zu gelangen, soll eine Geldzahlung erfolgen. Dieses wird meist in Form einer digitalen Währung eingefordert, auch Krypto-Währung genannt, wie beispielsweise Bitcoins. Dabei ist es nicht unüblich, dass der Bildschirm serviceorientiert ähnlich einer Dienstleistungswebsite aufgebaut ist und Informationen dazu enthält, was Bitcoins sind und wie diese erworben und transferiert werden können. Ferner bauen Täter teilweise zusätzlichen psychischen Druck durch die Ankündigung auf, dass sich die Zahlungsforderung erhöht, wenn die Transaktion nicht innerhalb eines bestimmten Zeitraums durchgeführt wird. Ob nach der Geldzahlung der Zugang zu den Daten wirklich wiederhergestellt wird, ist dabei ebenso ungewiss wie der Aspekt, ob weitere Schadsoftware auf dem System verbleibt und sich der Vorfall wiederholen wird. Ebenso besteht auch die Gefahr, dass zahlungsbereite Betroffene als solche von Tätern gelistet werden und somit das Risiko einer erneuten Viktimisierung erhöht sein könnte.

Ransomware-Angriffe können sowohl große Unternehmen als auch kleine Handwerksbetriebe oder Arztpraxen, genau wie Behörden und Privatnutzer treffen. Denn Kundendaten, Rechnungswesen, Kommunikation und vertrauliche Daten werden mittlerweile nahezu überall in Deutschland digital verwaltet. Die Größe des Schadens eines Ransomware-Angriffs hängt dabei u. a. von der Vertraulichkeit der Daten sowie der Tatsache, ob Sicherheitskopien (so genannte Backups) zur Verfügung stehen, ab.

1.4.4 (Distributed) Denial-of-Service

Beispiel: Ein Angriff auf das US-Unternehmen Dyn hat an der Ostküste der USA dazu geführt, dass für die Dauer von zwei Stunden zahlreiche Internetseiten, darunter auch populäre Onlinedienste wie twitter, amazon und netflix, nicht mehr zur Verfügung standen.[18] Bei Dyn handelt es sich um einen Vermittlungsdienst zwischen dem Aufrufen eines Domainnamens und dem jeweiligen Server und ermöglicht insofern die Bereitstellung der Onlinedienste. Der Ausfall kam jedoch nicht durch eine Schadsoftware zustande, sondern dadurch, dass innerhalb kürzester Zeit massenhafte Anfragen an den Server von Dyn geschickt wurden. Dadurch wurde das System überlastet. Für diese massenhaften Anfragen wurde ein Botnetz ge-

17 Da hierbei der Nutzer durch den (drohenden) Verlust seiner Daten psychisch unter Druck gesetzt werden soll, wird diese Angriffsart teilweise auch als *Scareware* bezeichnet.

18 https://www.zeit.de/digital/internet/2016-10/ddos-attacke-dyn-internet-der-dinge-us-wahl (aufgerufen am 4.1.2020).

nutzt (siehe oben). Interessanterweise beinhaltete dieses nicht nur die Rechenleistung vieler Computer, sondern auch von „smarten" Haushaltsgeräten, welche mit dem Internet verbunden sind, so genannte Internet of Things (dt.: Internet der Dinge).

Durch massenhafte Anfragen, die von fünf Botnetzen ausgingen, wurden die Internetseiten von Apple Daily und PopVote überlastet.[19] *Diese unterstützten 2014 die Demokratiebewegung Occupy Central in Hongkong.*

So genannte Denial of Service-Attacken (dt.: verteilte Blockade von Diensten; kurz: DoS-Attacke) zielen darauf ab, durch massenhafte Anfragen auf eine Webpräsenz zu einer Serverüberlastung dieser zu führen (siehe u. a. *Bundeskriminalamt*, 2019, S. 31-34). Distributed Denial of Service-Angriffe (kurz (D)DoS) stellen eine Spezifikation dar, bei der der Angriff von einer Vielzahl an Quellen ausgeht, wie beispielsweise durch ein Botnetz. Anders als bei der Verbreitung von Schadsoftware intendieren (D)DoS-Angriffe nicht, Daten zu verschlüsseln oder auszuspähen. Vielmehr soll ein Internetauftritt zerstört werden, wodurch in der Folge die jeweiligen Onlinedienste nicht mehr angeboten werden können. Ein (D)DoS-Angriff zielt darauf ab, eine Serverüberlastung herbeizuführen. Solche Überlastungen sind auch außerhalb von kriminellen Angriffen bekannt, beispielsweise, wenn ein städtisches Schwimmbad zu einem bestimmten Zeitpunkt die Anmeldemöglichkeit zu begehrten Schwimmkursen freistellt. Versuchen nun viele Eltern zu dem Anfangszeitpunkt ihren Wunschkurs für ihr Kind zu buchen, kommt es durch die massenhaften zeitgleichen Anfragen nicht selten auch zu (kurzfristigen) Serverüberlastungen.

(D)DoS-Angriffe nutzen zumeist dafür die oben beschriebenen Botnetze. Mittels dieser großen Rechenkapazität werden massenhaft Anfragen an eine Internetseite verschickt, z. B. durch das automatisierte Ausfüllen von Online-Formularen in großer Zahl, bis das System zusammenbricht. Dies hat die Konsequenz, dass Onlinedienste nicht mehr zur Verfügung gestellt werden können, was insbesondere für Online-Händler schon kurzzeitig zu großen finanziellen Verlusten führen kann.

(D)DoS-Attacken können auch mit weiteren Angriffsformen kombiniert auftreten. Dabei kann eine durchgeführte oder auch nur angedrohte (D)DoS-Attacke beispielsweise Bestandteil eines Ransomware-Angriffs sein, indem ein Lösegeld für die Beendigung bzw. das Ausbleiben einer solchen Tat gefordert wird.

1.4.5 Spyware

Beispiel: Ein überaus professioneller Täterkreis arbeitete eine Spionagesoftware aus, welche jahrelang in asiatischen Luxushotels verbreitet wurde.[20] *Während die Betroffenen mit dem WLAN des Hotels verbunden waren, bekamen sie Empfehlungen von scheinbaren Programmupdates. Durch die Aktivierung der Updates wurde eine Spionagesoftware heruntergeladen, welche den Angreifern ermöglichte, Passwörter und andere*

19 https://www.computerwoche.de/a/die-fuenf-bekanntesten-ddos-attacken-und-was-wir-aus-ihnen-lernen-koennen,3546023 (aufgerufen am 4.1.2020).

20 https://www.kaspersky.de/blog/darkhotel-spionage/4409/ (aufgerufen am 5.1.2020).

Daten auf den Computern auszuspähen. Mittels eines so genannten Keyloggers (engl., dt.: „Tasten-Protokollierer") konnten die Täter die Tastatureingaben der Betroffenen nachvollziehen.

Der Begriff Spyware (von engl. spying, dt.: spionieren) bezeichnet Programme, die dazu genutzt werden, einen illegalen Zugang zu Daten zu erlangen. Hierbei wird nicht darauf abgezielt, Daten zu verschlüsseln, zu zerstören oder anderweitig zu manipulieren, sondern Informationen zu erlangen, d. h. möglichst unbemerkt Daten auszuspionieren. Der betroffene Nutzer ist durch den ausschließlichen Einsatz von Spyware nicht in der Nutzung des Computers beeinträchtigt und dürfte so in vielen Fällen nichts bzw. nicht unmittelbar von dem Angriff mitbekommen.

Vorzufinden ist diese Bedrohungsform von Cyberkriminalität typischerweise im Bereich der so genannten Wirtschafts- bzw. Produktspionage. Daneben kann Spyware jedoch auch als Vorbereitungshandlung für weitere Cyberangriffe eingesetzt werden. So können Informationen über ein Unternehmen oder eine Behörde auch dazu dienen, im weiteren Verlauf manipulativ auf Menschen einzuwirken und sie dadurch zu bestimmten Handlungen zu bewegen, wie beispielsweise im Kontext des „Chef-Betrugs" bzw. „CEO-Fraud" (so genanntes *social engineering*, siehe unten).

1.4.6 Social Engineering

Beispiel: Der Nürnberger Kabelhersteller Leoni wurde Opfer eines Cyberangriffs, der nicht mittels Schadsoftware ausgeführt wurde.[21] *Statt auf die IT-Technik einzuwirken, hatten die Täter Mitarbeiter der Buchhaltung im Visier. Mit diesen nahmen sie per E-Mail Kontakt auf, wobei diese so präpariert waren, dass sie den Anschein erweckten, sie stammten von bestimmten Mitarbeitern, insbesondere solche in Führungspositionen, des Unternehmens. Die Täter suggerierten demnach, Positionen in der Firma innezuhaben, die sie berechtigten, bestimmte Finanztransaktionen bei der Buchhaltung zu veranlassen. Der Schaden für das Unternehmen belief sich auf ca. 40 Millionen Euro.*

Das so genannte *social engineering* bezeichnet einen Phänomenbereich, bei dem manipulativ auf einen Menschen eingewirkt wird. Vergleichbar mit einem Betrugsdelikt wird die jeweilige Zielperson unter Vorspiegelung falscher Tatsachen dazu veranlasst, bestimmte Handlungen auszuführen, welche dem Täter einen Vorteil verschaffen. Insofern existierten Straftaten, die auf *social engineering* basieren, schon vor der Entwicklung des Internets. Begünstigt wird die soziale Manipulation, wenn Täter und Opfer nicht persönlich aufeinandertreffen. So erfolgten in den 1980er Jahren beispielsweise Angriffe auf Telefongesellschaften mit dem Ziel, Passwörter zur Herstellung von Telefonverbindungen zu erlangen (*Büchel/Hirsch*, 2014, S. 17). Das digitale Zeitalter schafft dem Tatvorgehen im Sinne des *social engineerings* eine breitere Verwendung. Vor allem größere Unternehmen sind hiervon betroffen (siehe dazu Kapitel 3 im

21 https://www.handelsblatt.com/unternehmen/industrie/leoni-trickdiebe-erleichtern-zulieferer-um-millionen/14019400.html (aufgerufen am 5.1.2020).

vorliegenden Band), ebenso können aber auch Behörden und Privatnutzer zum Opfer eines *social engineerings*-Angriffs werden.

Eine bekannte Form des *social engineerings* stellt der so genannte Chefbetrug dar, auch mittels der englischen Bezeichnung für den Geschäftsführer/-leiter (Chief Executive Officer) als CEO-Fraud bezeichnet. Typischerweise hat sich der Täter hierbei im Vorfeld zur eigentlichen Tat Informationen über das Unternehmen beschafft. Hierbei kann es sich einerseits um frei zugängliche Daten handeln, wie beispielsweise eine Organigramm-Übersicht des Unternehmens oder weitere Angaben, welche der Internetpräsenz entnommen werden können. Ferner kann der Täter aber auch durch den Einsatz von Spyware (siehe oben) Informationen erlangt haben. Diese dienen dem Täter dann in einem weiteren Schritt dazu, sich als Führungskraft des Unternehmens gegenüber einem Unternehmensmitarbeiter auszugeben. Die anvisierte Person kennzeichnet, dass sie monetäre Transaktionen des Unternehmens auslöst, beispielsweise indem sie in der Buchhaltung tätig ist, oder anderwärtig Zugang zu Daten hat, die für den Täter von Interesse sind. So können auch Personen aus der IT-Abteilung für den Täter interessant sein, wenn es sich beispielsweise um das Erlangen von Zugangspasswörtern handelt. Mittels E-Mails tritt der Täter nun in die Kommunikation mit der Zielperson ein und fordert diese unter Vorspiegelung, sein Vorgesetzter zu sein, dazu auf, Geldzahlungen auf ein bestimmtes Konto zu veranlassen.

Das Ausüben von psychischem Druck durch Betonung von Vertraulichkeit und Dringlichkeit unterstützt das manipulative Einwirken. Ebenso die Tatsache, dass es sich, zumindest aus Sicht des Betroffenen, um eine Autoritätsperson handelt, dessen Anweisungen man Folge zu leisten hat. Die Bitte um Verschwiegenheit und das Hervorheben des Umstands, es handele sich um ein äußerst wichtiges Geschäft für das Unternehmen, führt auch zu einer Aufwertung der Arbeit des Betroffenen und damit verbundenen Gefühlen der Wertschätzung.

Typischerweise sind Tathandlungen wie der Chefbetrug keine Massenangriffe, die sich gleichzeitig auf viele Internetnutzer beziehen. Um für den Täter erfolgreich zu verlaufen, müssen diese zielgerichtet ausgeübt werden und setzen insofern Vorbereitungshandlungen wie das Einholen von Informationen über das Unternehmen, die einzelnen Mitarbeiter, die Kommunikationskultur oder auch der Zeitpunkt von bestimmten Unternehmensereignissen wie beispielsweise Auslandsreisen voraus.

Zur Ausübung eines social engineering-Angriffs kann auch Spyware oder Schadsoftware eingesetzt werden. Allerdings kennzeichnet diese Bedrohungsform, dass sie weniger durch das Versagen von IT-technischen Sicherheitsmaßnahmen wie Firewalls und Antivirenscannern gelingt, sondern durch den so genannten „Risikofaktor Mensch". Es sind weniger IT-Systeme, auf die der Täter unrechtmäßig einwirkt, als auf Mitglieder von Organisationen, und diese zu den jeweiligen Handlungen veranlasst. Dieses Grundelement findet sich auch in einigen anderen Arten von Cyberkriminalität, wie beispielsweise in Form der oben angesprochenen Mail, welche eine Schadsoftware im Anhang enthält, jedoch den Anschein einer gängigen Rechnungszustellung suggeriert. Ferner ist social engineering auch ein essenzieller Bestandteil von so genannten Phishing-Angriffen.

1.4.7 Phishing

Beispiel: Massenhaft versandte E-Mails mit dem Betreff „Ihr Konto wurde eingeschränkt" gaben den Anschein, es handele sich um eine Nachricht vom Unternehmen Amazon an einen Kunden.[22] In der E-Mail wird erläutert, dass eine Sicherheitskontrolle durchgeführt und die Daten innerhalb von 48 Stunden verifiziert werden müssten. Dazu wird der Empfänger der E-Mail aufgefordert, auf das Feld „Weiter zur Verifizierung" zu klicken. Dadurch wird der Betroffene auf eine gefälschte Internetseite weitergeleitet, die den Anschein macht, ein Anmeldeportal von Amazon zu sein. Durch die Eingabe der persönlichen Zugangsdaten gelangen diese zu den Tätern, welche infolgedessen u. a. in der Lage sind, auf Kosten des Accountinhabers Waren zu bestellen.

Phishing-Angriffe (zusammengesetzt aus „P" wie Passwort und „fishing" im Sinne von Fischen bzw. Abschöpfen) zielen auf die Erlangung von sensiblen Daten, wie beispielsweise Zugangsdaten zu Bankkonten, Kreditkartendaten, Passwörtern und ähnliches ab (*Wernert*, 2014, S. 136-138). Anders als bei dem Einsatz von Spyware erlangt der Täter die Informationen jedoch nicht durch das alleinige Ausspionieren, sondern durch das Zutun des Betroffenen. Ein verbreitetes Tatvorgehen im Kontext von Phishing ist das (massenhafte) Versenden von E-Mails, welche vorgeben, die Bank würde sich wegen eines wichtigen Anliegens, z. B. eines Sicherheitsvorfalls, an den jeweiligen Kunden wenden. Der Betroffene wird aufgefordert, einem Link zu folgen und so die scheinbare Internetseite der Bank zu öffnen und sich bei seinem Online-Banking-Account anzumelden. Hierbei handelt es sich jedoch um eine der echten Webpräsenz der Bank nur nachempfundene Internetseite. Durch die Eingabe der Zugangsdaten gelangen die vertraulichen Daten zu dem Täter. Die Variationen vom Tatvorgehen im Zusammenhang mit Phishing-Angriffen sind zahlreich. So kann etwa auch Schadsoftware eingesetzt werden, welche durch das Aufrufen der jeweiligen Internetseite auf das Computersystem gelangt (*Wernert*, 2014, S. 136). Hierbei werden beispielsweise Posts in sozialen Netzwerken eingesetzt, die suggerieren, von bekannten Herstellern zu sein. Wird dieser angeklickt, landet der Nutzer jedoch auf einer gefälschten Internetseite, die der Originalseite hinsichtlich des Firmenlogos und der Gestaltung sehr ähnlich ist. Allerdings ist in der Adresse im Browser erkennbar, dass es sich nicht um die Originalseite handelt. Insofern ist es bei Weiterleitungen ratsam, auf die Browserzeile zu achten (Näheres zu Sicherheitsmaßnahmen siehe Kapitel 11 im vorliegenden Band).

Das Abgreifen individueller Zugangsdaten wird auch digitaler Identitätsdiebstahl genannt (*Bundeskriminalamt*, 2019, S. 17), da der Täter sich durch die Daten online als jemand anderes ausgeben kann und den Betroffenen somit quasi seiner Identität beraubt. Dabei ist Phishing nicht nur auf den Bereich des Online-Banking beschränkt, sondern kann auch in Bezug auf andere Zugangsdaten gegeben sein.

---

22 https://www.bsi-fuer-buerger.de/BSIFB/DE/Risiken/SpamPhishingCo/Phishing/BeispielePhishingAngriffe/beispielephishingangriffe_node.html (aufgerufen am 5.1.2020).

Wie bei den vorherig aufgeführten Bedrohungsformen von Cyberkriminalität kann auch das Phishing in Verbindung mit anderen Angriffsarten auftreten. Insbesondere sind hierbei Überschneidungen mit dem Phänomen des *social engineerings* gegeben, da das manipulative, unter Vorspiegelung falscher Tatsachen basierte Einwirken auf eine Person, um sie zu bestimmten Handlungen zu veranlassen, auch ein Grundelement des Phishings ist.

1.4.8 Weitere Angriffsarten

Wie schon mehrfach hingewiesen, gibt es eine Vielzahl verschiedener Bezeichnungen und Unterkategorien der zuvor genannten Angriffsarten. Dies ist nicht nur der Komplexität des Gegenstands geschuldet, sondern auch der starken Dynamik im IT-Bereich. Digitale Anwendungen werden erweitert, neue kommen hinzu und auf bisherige Schwachstellen wird durch erweiterte Sicherheitsmaßnahmen reagiert. Auf diese Veränderungen reagieren Täter und kombinieren vorhandene und entwickeln neue Angriffsarten. Dennoch grenzen die zuvor dargestellten Bedrohungsformen die Grundelemente verschiedener Cyberangriffe voneinander ab und stellen insofern Grundkategorien und -typen der Bedrohung dar, mittels derer sich der Phänomenbereich der Cyberkriminalität analysieren und beschreiben sowie untersuchen lässt. Auf einige der denkbaren Überschneidungen und Verflechtungen dieser Angriffsformen untereinander wurde an verschiedener Stelle bereits hingewiesen.

Die Pluralität von Begriffen im Zusammenhang mit Cyberkriminalität hängt sicher auch mit dem Fehlen einer Standardisierung in diesem Feld zusammen. Andere Deliktsbereiche korrespondieren stärker mit den Einordnungen des Strafgesetzbuchs und verfügen so über angemessene Definitionen. Im Kontext von Cyberkriminalität führt die Anzahl von Sonderformen zu einer Vielzahl an Begrifflichkeiten. Hierzu sei als Beispiel das so genannte Defacing genannt. Defacing stellt eine Sonderform in der Folge eines Angriffs zum Beispiel mittels einer Schadsoftware dar und zielt darauf ab, den Internetauftritt des Betroffenen zu verändern. Motive für ein solches Vorgehen können in dem Willen, politische oder religiöse Botschaften zu verbreiten, liegen oder um eigene Handlungsmacht zu demonstrieren.

Neben den genannten Bedrohungsformen sei jedoch auf eine weitere Variante hingewiesen, welche sich von den bisherigen Angriffsformen unterscheidet und insbesondere für Behörden und Unternehmen ein Risiko darstellt: das so genannte manuelle Hacking (*Dreißigacker et al.*, 2020). Hierbei greift der Täter gezielt auf Software, Hardware oder Daten zu, um z. B. Konfigurationen zu verändern, Einsicht in Daten zu erlangen oder diese zu löschen, nutzt dafür jedoch keine sich automatisch verbreitende Schadsoftware oder eine andere der oben aufgeführten Begehungsarten. Vielmehr hat der Täter Zugang zu den Computern und kann dadurch den Angriff ausführen, indem er beispielsweise unautorisierte Konfigurationen oder Manipulation an Hardware durchführt. Neben Personen, die sich unautorisiert Zugang zu dem jeweiligen Gebäude verschafft haben, kommen in diesem Zusammenhang hauptsächlich Mitarbeiter bzw. ehemalige Mitarbeiter in Frage, aber auch Besucher der Behörde. Ursächlich für die schädigende Absicht einer Person, die der jeweiligen Organisation angehört, könnte neben dem Motiv der eigenen Vorteilsverschaffung auch Rache

aufgrund einer vorherigen Verwerfung mit dem Arbeitgeber sein (siehe Kapitel 2 im vorliegenden Band).

1.5 Fazit

Anders als bei anderen Deliktsbereichen korrespondieren Angriffe aus dem Bereich Cyberkriminalität nicht unbedingt mit Straftatsnormen des Strafgesetzbuchs. Vielmehr ist Cyberkriminalität durch eine Vielzahl unterschiedlicher Begriffe gekennzeichnet, welche zudem teilweise verschieden definiert werden. Dies liegt einerseits an der Vielzahl sehr unterschiedlicher Herangehensweisen und Perspektiven auf den Phänomenbereich, andererseits sicherlich auch an der Beliebtheit des Präfix *Cyber*, wodurch immer wieder neue Wortbildungen kreiert werden. Ziel des vorliegenden Kapitels war es insofern, die verschiedenen Begriffe und Kategorisierungen, die in dem Kontext Cyberkriminalität verwandt werden, zu erläutern und zu definieren. Dabei zeigte sich, dass die verbreitete Unterscheidung von Cyberkriminalität im weiteren und engeren Sinn nur bedingt brauchbar erscheint. Vielmehr adressieren eine Vielzahl an Angriffsarten beide Bereiche, wie beispielsweise ein Ransomware-Angriff.

Ferner weisen die dargestellten Bedrohungsformen sowohl Angriffe auf, die sehr gezielt eine bestimmte Behörde anvisieren als auch solche, die breit gestreut sind und eine Vielzahl von Nutzern treffen können. Nicht immer sind es technische (Sicherheits-)Lücken, die einen Cyberangriff ermöglichen, in vielen Fällen kommt es vielmehr (auch) auf das Verhalten der Mitarbeiter an, in dem diese beispielsweise einen Anhang mit Schadsoftware öffnen. Dies zeigt, dass neben technischen (siehe hierzu u. a. Kapitel 11 im vorliegenden Band) auch organisatorische Sicherheitsmaßnahmen notwendig sind, die die Mitarbeiter der Behörde adressieren (siehe hierzu Kapitel 12 im vorliegenden Band). Ferner ist die Diversität von Bedrohungsformen jedoch auch ein Hinweis dafür, dass Täter nicht ausschließlich gezielt vorgehen und insofern prinzipiell jede Behörde von Cyberkriminalität betroffen sein kann.

1.6 Literatur

Agrafiotis, Ioannis/Nurse, Jason R. C./Goldsmith, Michael/Creese, Sadie/Upton, David, A taxonomy of cyber-harms, Journal of Cybersecurity 4(1), 2018, S. 1-15.

Bergmann, Mare C./Baier, Dirk, Prevalence and Correlates of Cyberbullying Perpetration. Findings from a German Representative Student Survey, International Journal of Environmental Research and Public Health 15(2), 2018, S. 274-287.

Bergmann, Marie C./Dreißigacker, Arne/von Skarczinski, Bennet/Wollinger, Gina R., Cyber-Dependent Crime Victimization: The Same Risk for Everyone? Cyberpsychology, Behavior, and Social Networking, 21(2), 2018, S. 84-90.

Bergmann, Marie C./Kliem, Sören/Krieg, Yvonne/Beckmann, Laura, Jugendliche in Niedersachsen. Ergebnisse des Niedersachsensurveys. Forschungsbericht Nr. 144, Kriminologisches Forschungsinstitut Niedersachsen e.V., Hannover 2019, S. 44-50.

Büchel, Michael/Hirsch, Peter, Internetkriminalität, Heidelberg 2014.

Bundesamt für Sicherheit in der Informationstechnik (Hrsg.), Leitfaden zur Basis-Absicherung nach IT-Grundschutz. In drei Schritten zur Informationssicherheit, Bonn 2017.

Bundeskriminalamt, Cybercrime. Bundeslagebild 2018, Wiesbaden 2019.

Dahmen, Ulla/Krämer, Nicolas, Angriff aus der Dunkelheit: Cyberattacke auf das Lukaskrankenhaus Neuss, in Bartsch, Michael/Frey, Stefanie (Hrsg.), Cybersecurity Best Pracitces. Lösungen zur Erhöhung der Cyberresilienz für Unternehmen und Behörden, Wiesbaden 2018, S. 13-21.

Dreißigacker, Arne/von Skarczinski, Bennet/Wollinger, Gina R., Cyberangriffe gegen Unternehmen in Deutschland. Ergebnisse einer repräsentativen Unternehmensbefragung 2018/2019, Forschungsbericht Nr. 152, Kriminologisches Forschungsinstitut Niedersachsen e.V., Hannover 2020.

European Union Agency For Network And Information Security, ENISA Threat Taxonomy, A tool for structuring threat information, abrufbar unter: https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/threat-taxonomy/view (25.1.2020), 2016.

Harringer, Claus, „Good Bot, Bad Bot?" Zur Problematik von Bot-Ontologien, Information. Wissenschaft & Praxis, 69(5-6), 2018, S. 257-264.

Howard, John D./Longstaff, Thomas A., A Common Language for Computer Security Incidents, Sandia National Laboratories, Springfield, abrufbar unter: https://prod-ng.sandia.gov/techlib-noauth/access-control.cgi/1998/988667.pdf (25.1.2020), 1998.

Huber, Edith, Cybercrime. Eine Einführung, Wiesbaden 2019.

Hutchins, Eric M./Cloppert, Michael J./Amin, Rohan M., Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chaince. Abrufbar unter: https: // www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf (24.1.2020), 2010.

Information Security Forum, Information Risk Assessment Methodology 2 (IRAM), Executive Report Reference: ISF 17 07 02, 2017.

Jiang, Wei/Tian, Zhi-hong/Cui, Xiang, DMAT: A New Network and Computer Attack Classification 5(6), 2013, S. 101–106.

Jaishankar, Karuppannan, Cyber Criminology: Evolving a novel discipline with a new journal, International Journal of Cyber Criminology 1(1), 2007, S. 1-6.

Jouini, Mouna/Rabai, Latifa Ben Arfa/Aissa, Anis Ben, Classification of Security Threats in Information Systems, Procedia Computer Science 32, 2014, S. 489–496.

Klipper, Sebastian, Cyber Security, Wiesbaden 2015.

McGuire, Mike/Dowling, Samantha, Cyber crime: A review of the evidence. Summary of key findings and implications. United Kingdom, Home Office (Research Report, 75), 2013.

Nickerson, Robert C./Varshney, Upkar/Muntermann, Jan, A method for taxonomy development and its application in information systems, European Journal of Information Systems 22(3), 2013, S. 336–359.

Paoli, Letizia/Visschers, Jonas/Verstraete, Cedric, The impact of cybercrime on businesses: a novel conceptual framework and its application to Belgium, Crime Law Soc Change 70 (4), 2018, S. 397–420.

Rid, Thomas, Maschinendämmerung. Eine kurze Geschichte der Kybernetik, Berlin 2016.

Rüdiger, Thomas-Gabriel/Bayerl, Petra S. (Hrsg.), Cyberkriminologie. Kriminologie für das digitale Zeitalter, Wiesbaden 2020.

Simmons, Chris/Ellis, Charles/Shiva, Sajjan/Dasgupta, Dipankar/Wu, Qishi, AVOIDIT: A Cyber Attack Taxonomy, Annual Symposium on Information Assurance (9), 2014.

Steffens, Timo, Auf der Spur der Hacker, Berlin 2018.

Stiller, Anja/Boll, Lukas/Kretschmer, Saskia/Wollinger, Gina R./Dreißigacker, Arne, Cyberangriffe in Deutschland. Ergebnisse einer qualitativen Expertenbefragung, KFN-Forschungsbericht Nr. 155, Hannover 2020 (in press).

Thiedeke, Udo, Cyberspace: Die Matrix der Erwartungen, in Thiedeke, Udo (Hrsg.), Soziologie des Cyberspace. Medien, Strukturen und Semantiken, Wiesbaden 2004, S. 121-143.

Wernert, Manfred, Internetkriminalität, Stuttgart 2014.