WERNERT

Internetkriminalität

Grundlagenwissen, erste Maßnahmen und polizeiliche Ermittlungen

4. Auflage

BOORBERG

Internetkriminalität

Grundlagenwissen, erste Maßnahmen und polizeiliche Ermittlungen

Manfred Wernert
Erster Kriminalhauptkommissar
Hochschule für Polizei Baden-Württemberg
Institutsbereich Ausbildung Lahr

4., aktualisierte Auflage, 2021

BOORBERG

Bibliografische Information der Deutschen Nationalbibliothek |
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über www.dnb.de abrufbar.

4. Auflage, 2021

ISBN 978-3-415-06891-9 E-ISBN 978-3-415-06892-6
E-Book-Umsetzung: Datagroup int. SRL, Timisoara
© 2011 Richard Boorberg Verlag
Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung, die nicht ausdrücklich vom Urheberrechtsgesetz zugelassen ist, bedarf der vorherigen Zustimmung des Verlages. Dies gilt insbesondere für Vervielfältigungen, Bearbeitungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.
Satz: abavo GmbH, Nebelhornstraße 8, 86807 Buchloe | Druck und Bindung: Laupp & Göbel GmbH, Robert-Bosch-Straße 42, 72810 Gomaringen

Richard Boorberg Verlag GmbH & Co KG | Scharrstraße 2 | 70563 Stuttgart
Stuttgart | München | Hannover | Berlin | Weimar | Dresden
www.boorberg.de

Inhaltsverzeichnis

Vorwort 4. Auflage 9

Vorwort 3. Auflage 11

Vorwort 2. Auflage 13

Vorwort 1. Auflage 15

Abkürzungsverzeichnis 17

1 Missbrauchspotenzial Internet 19

2 Kriminalitätsbegriff 32
2.1 Kriminalitätsmerkmale 32
2.2 Begriff Cybercrime 33
2.3 Cybercrime im engeren Sinn 35
2.3.1 Straftaten nach dem Strafgesetzbuch (StGB) 36
2.3.2 Urheberrechtsverletzungen, Softwarepiraterie – Gesetz über Urheberrecht und verwandte Schutzrechte (UrhG) 37
2.3.3 Verstöße gegen das Telekommunikationsgesetz (TKG) . . 37
2.4 Cybercrime im weiteren Sinn. 38
2.5 Täterstruktur 38
2.6 Kriminologische Einordnung 40

3 Polizeiorganisation und Strategie 43
3.1 Internetwache 44
3.2 Internetrecherche/Streife im Netz 45
3.3 Sachbearbeitung 46
3.4 Spezialdienststellen/Kompetenzzentren 48
3.5 Personelle Auswirkungen und technische Ausstattung 52
3.6 Rechtsgrundlagen 56
3.6.1 Ermittlungsrelevante Daten. 57
3.6.2 Bedeutung der Grundrechte 58
3.6.3 Urteil des Bundesverfassungsgerichts zur Online-Durchsuchung 59
3.6.4 Rechtsgrundlagen zur Datenermittlung 62
3.6.5 Rechtsgrundlagen im Überblick 67
3.6.6 Rechtsgrundlagen zur Fahndung, Durchsuchung und Beschlagnahme. 70

3.7 Prävention 72
3.8 Grenzüberschreitende Bekämpfung/Kooperationen 78
3.9 Staatsanwaltschaft 83

4 IT-Technik 86
4.1 Hardware 86
4.2 Software 88

5 Internet 91
5.1 Entwicklung 91
5.2 Begriff und Funktionsweise 92
5.3 Datentransfer 93
5.4 Verschlüsselungstechnik 95

6 Tatgelegenheit WLAN 97
6.1 Modus Operandi 97
6.2 WarDriving 98
6.3 WarChalking 99
6.4 Rechtsverstöße und Maßnahmen 100

7 Tatmittel E-Mail 102

8 Ermittlungen zur IP-Adresse 106

9 Ermittlungen zur DOMAIN 112

10 Sicherstellung elektronischer Beweismittel 117
10.1 Spezielle Aspekte bei der Wohnungsdurchsuchung 119
10.2 Sicherung einer EDV-Anlage 124
10.3 Netzwerke 133
10.4 Scanner/Drucker/Kombigeräte 135
10.5 Digitalkamera 136
10.6 Multimediale Unterhaltungsgeräte 136
10.7 Mobilfunktelefon 136
10.8 PDA und Co. 139
10.9 Asservierung/Untersuchungsantrag 140

11 Happy Slapping/SNUFF-Video 142

12 Kinderpornografische Schriften 144

13 Betrug bei Internetauktionen 148

14 Urheberrechtsverletzungen 151

15 Diebstahl digitaler Identitäten 154
15.1 Carding 156
15.2 Phishing 157
15.3 Skimming 161

16 Digitale Erpressung 164

17 Botnetz 169

18 Soziale Netzwerke 174

19 Ermittlungshilfe Internet 180

20 Anhang 184
20.1 Strafgesetzbuch (Auszug) 184
20.2 Gesetz über Urheberrecht und verwandte Schutzrechte (Auszug) 188
20.3 Telekommunikationsgesetz (Auszug) 192
20.4 Telemediengesetz (Auszug) 204
20.5 Strafprozessordnung (Auszug) 207
20.6 Online-Angebote mit Fachinformationen und zur Prävention . . 223

Glossar 227

Stichwortverzeichnis 233

Vorwort 4. Auflage

Die tagesaktuelle Berichterstattung verdeutlicht die Brisanz der Internetkriminalität. Betrugshandlungen, Kinderpornografie, strafbewehrte Selbstinszenierung in Internetforen und professionelle Hacker bestimmen die Schlagzeilen und beeinträchtigen das Sicherheitsgefühl in der Öffentlichkeit. Rasante technische Entwicklungen leisten dem Missbrauch Vorschub. Der Gesetzgeber tut sich schwer, mit rechtlichen Anpassungen hier Schritt zu halten. Umso mehr ist die Polizei gefordert, um mit den ihr zur Verfügung stehenden Mitteln und Möglichkeiten einen maßgeblichen Beitrag zur Bekämpfung der Internetkriminalität zu leisten. Hier ist es notwendig, bundesweit und über Landesgrenzen hinweg zusammenzuarbeiten. Auch im gemeinsamen Agieren mit außerpolizeilichen Organisationen und Einrichtungen sind Synergieeffekte zu erzielen.

Innerhalb dieser Dimensionen sind jede Polizeibeamtin und jeder Polizeibeamte gehalten, sich zum Kriminalitätsphänomen zu orientieren. Zur erfolgreichen Abwehr von Gefahren und der Verfolgung und Aufklärung von Straftaten ist eine angemessene Basiskompetenz gefordert.

Das vorliegende Buch soll hierzu seinen Beitrag leisten. Daneben bietet es eine Schnittstelle zu weitergehenden Informationen, Spezialgebieten und Ermittlungsmöglichkeiten.

Lahr, im November 2020 Manfred Wernert

Vorwort 3. Auflage

Es geht weiter. Das Internet ist allseitig, das „Allesnetz“ ist angesagt. Immer mehr durchdringt die Digitalisierung die Tageswelt. Und natürlich bieten die neuesten technischen Möglichkeiten und die weitgehende Verbreitung und Nutzung der Datennetze auch neue Tatgelegenheiten. Wo Menschen sind, da „menschelt's!“, oder nach frühester kriminologischer Erkenntnis – „Verbrechen ist ubiquitär“ – Kriminalität ist überall – so auch im Netz.

Sicherheit hat auch hier ihren Preis. Es bleibt die Frage, was es uns wert ist und welche Grundvoraussetzungen wir schaffen, um Sicherheit zu gewährleisten – Umsicht und Weitblick von Verantwortungsträgern sind gefragt. Dazu gehört nachhaltiges Agieren und nicht bloß überhastetes Reagieren, purer Aktionismus. Neben den vielen sich bietenden Chancen des Internets bedarf es des geschärften Blickes und der angemessenen, aber deutlichen Reaktion bei Fehlentwicklungen.

Zwischen unkontrollierter, globalisierter Netzfreiheit und Cyber-Nato bewegen sich die Sicherheitsbehörden und letztlich auch die Polizei.

Gerade sie ist auf solide Ressourcen angewiesen. Aktuellste Technik und bestqualifizierte Kräfte bilden maßgeblichen Anteil, um dem gesteigerten Sicherheitsbedürfnis in der Gesellschaft Rechnung zu tragen.

Dabei sind nicht nur die Spezialdienststellen, sondern gerade jede Polizeibeamtin und jeder Polizeibeamte tagtäglich in diesem Kriminalitätsbereich gefordert. Augenmaß und Handlungssicherheit stellen hier wichtige Grundpfeiler für die ersten Feststellungen und Maßnahmen zur Abwehr von Gefahren und der Verfolgung und Aufklärung von Straftaten dar.

Das Buch versteht sich dafür auch weiterhin als übersichtlicher und verständlicher Beitrag für die Praxis und die polizeiliche Aus- und Fortbildung.

Lahr, im Februar 2017 Manfred Wernert

Vorwort 2. Auflage

Die Informations- und Kommunikationstechnik entwickelt sich exponentiell und die Kriminalitätsentwicklung geht mit den technischen Möglichkeiten einher. Das Internet bildet dafür die Plattform und birgt neben den vielen Chancen auch enorme Risiken. Im Spannungsfeld von Freiheit und Sicherheit ist es auch Aufgabe der Kriminalistik, Angriffe auf die Integrität informationstechnischer Systeme abzuwehren und Straftaten beweissicher zu verfolgen. Nur dann kann dem ausgeprägten Sicherheitsbedürfnis der Bevölkerung in diesem Bereich Rechnung getragen werden. In Abgrenzung zu den Geheimdiensten orientieren sich die Strafverfolgungsbehörden, allen voran die Polizei, bei der Erfüllung ihres Auftrages an einem verantwortlichen Umgang mit unserer Verfassung und den darin verankerten Grundrechten.

Neben einer umfassenden Aufklärung im Sinne der Prävention bedarf es der ständigen Fortentwicklung personeller und technischer Ressourcen zur Kriminalitätsbekämpfung. Neben klassischen kriminalistischen Tugenden sind fachspezifische Kenntnisse für den mit Internetkriminalität konfrontierten Polizeibeamten gefordert. Das Buch liefert dafür die Kerninformationen zu den aktuellen Erscheinungsformen dieses Kriminalitätsbereiches, den rechtlichen Grundlagen und kriminalistischen Möglichkeiten. Es soll weiterhin als strukturierter Beitrag für die Praxis und die polizeiliche Aus- und Fortbildung dienen.

Lahr, im März 2014 Manfred Wernert

Vorwort 1. Auflage

Der Einzug von Computern in nahezu alle Bereiche des gesellschaftlichen Lebens, die steigende Anzahl der Internetnutzer und die damit einhergehenden aktuellen Kriminalitätsentwicklungen führen auch für die Aufgaben der Polizei zu Veränderungen.

Die Polizei muss dem Bürger bei der Anzeigenaufnahme auch in diesem Deliktsbereich ein kompetenter Ansprechpartner sein.

Mit der **Anzeigenaufnahme** und der **Durchführung des Ersten Angriffs** sind unter anderen regelmäßig die **Polizeibeamtinnen und -beamten des Streifendienstes** und **der Bezirks- und Postendienste** konfrontiert. Die **Fortentwicklung** der **Kriminalistik** ist in diesem Zusammenhang notwendiger denn je.

Die Anzeigenaufnahme und die Bearbeitung von Delikten im Zusammenhang mit der Informations- und Kommunikationstechnik erfordern **fachspezifische Kenntnisse.**

Ziel der Behandlung des Themas in diesem Buch ist es insbesondere, dem mit diesen Aufgaben befassten Kollegenkreis entsprechende **Informationen** zu **vermitteln.**

Dabei geht es um das allgemeine Verständnis des **Kriminalitätsphänomens, rechtliche Entwicklungen**, die **Vornahme relevanter Feststellungen** und die sachgerechte **Sicherung elektronischer Beweismittel** als Bedingungen einer optimalen Auswertung durch qualifizierte Sachbearbeiter.

Analog dem Ergebnis klassischer Tatortarbeit soll auch die **Sicherung digitaler Spuren** den forensischen Anforderungen entsprechen.

Mit als **Basis** der Empfehlungen dienten **die aktuellen Handlungsanweisungen der Landeskriminalämter** und Erfahrungen der Praxis.

Das Buch soll damit einen **strukturierten Beitrag** zur geforderten Vermittlung des Grundlagenwissens und den Herausforderungen an die Strafverfolgungsbehörden im Bereich der Bekämpfung der Kriminalität mit Informations- und Kommunikationsmedien im Rahmen der **polizeilichen Aus- und Fortbildung** leisten.

Lahr, im Februar 2011 Manfred Wernert

Abkürzungsverzeichnis

APRAnet	Advanced Research Project Agency NETwork
BBK	Bundesamt für Bevölkerungsschutz und Katastrophenhilfe
BfV	Bundesamt für Verfassungsschutz
BITKOM	Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.
BKA	Bundeskriminalamt
BMJV	Bundesministerium für Justiz und für Verbraucherschutz
BND	Bundesnachrichtendienst
BNetzA	Bundesnetzagentur
BPOL	Bundespolizei
BSI	Bundesamt für Sicherheit in der Informationstechnik
BVerfG	Bundesverfassungsgericht
CERN	Centre Européen de Recherches Nucléaires
DNS	Domain Name Systems
GiV	Gefahr im Verzug
GSM	Global System für Mobile Communications
http-Protokoll	HypertextTransferProtocol
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
IKZ	Internet Kompetenz Zentrum
IM	Innenministerium
IMK	Innenministerkonferenz
IMSI	International Mobile Subscriber Identity
Internet	InterconnectedNetworks
JMStV	Jugendmedienschutz-Staatsvertrag
LKA	Landeskriminalamt
LAN	LokalAreaNetwork
LTE	Long Term Evolution
KJM	Kommission für Jugendmedienschutz der Landesmedienanstalten
noeP	nicht offen ermittelnder Polizeibeamter
NotRufV	Notrufverordnung
PIN	Personal Identification Number
ProPK	Programm Polizeiliche Kriminalprävention der Länder und des Bundes
PUK	PIN Unblocking Key
SIM	Subscriber Identity Modul

SNS	Social network services
TCP/IP-Protokoll	TransmissionControlProtocol/InternetProtocol
TKG	Telekommunikationsgesetz
TMG	Telemediengesetz
TOR	The Onion Routing
UCE	Unsolicited Commercial E-Mails
UMTS	Universal Mobile Telecommunations System
UrhG	Gesetz über das Urheberrecht und verwandte Schutzrechte
URL	Uniform Resource Locator (deutsch: einheitlicher Quellenanzeiger oder Adresszeile)
VE	Verdeckter Ermittler
WLAN	WirelessLokalAreaNetwork
ZIT	Zentralstelle zur Bekämpfung der Internetkriminalität
ZKA	Zollkriminalamt

1 Missbrauchspotenzial Internet

Die Digitalisierung hat die Vernetzung der Welt erheblich beeinflusst und die Globalisierung auf eine neue Stufe gehoben. Ein Ende dieser Entwicklung ist nicht in Sicht. Genauso wie man Kleidung online kauft, kann man auch Drogen oder Waffen in der Underground Economy erwerben. Man findet im World Wide Web die Anleitung zum Aufbau eines Schrankes genauso wie die zum Bau einer Bombe. Und so praktisch Onlinebanking oder der smarte Backofen auch sind – sie bieten auch Angriffsmöglichkeiten für Straftäter.[1]

In seiner Rede anlässlich des Tages der Deutschen Einheit 2013 beschäftigte sich der damalige Bundespräsident Joachim Gauck mit den Chancen und Risiken dieser „**digitalen Revolution**“: „So wie einst die industrielle Revolution verändert heute die digitale Revolution unsere gesamte Lebens- und Arbeitswelt. Digitale Technik dient als Spielwiese, als Chatraum und ersetzt den Gang zur Bank. Freiwillig und gedankenlos geben Menschen bei jedem Klick ins Netz Persönliches preis, manche vertrauen sozialen Netzwerken sogar ihr ganzes Leben an – Ausgeliefertsein und Selbstauslieferung sind kaum voneinander zu trennen“, so der Bundespräsident.

Er beklagt die **schwindende Privatsphäre** und erkennt, dass Öffentlichkeit viele nicht mehr als Bedrohung empfinden, sondern als Verheißung, die Wahrnehmung und Anerkennung verspricht. „Sie verstehen nicht oder sie wollen nicht wissen, dass sie so mitbauen an einem digitalen Zwilling ihrer realen Person, der neben ihren Stärken eben auch ihre Schwächen enthüllt – oder enthüllen könnte. Der ihre Misserfolge und Verführbarkeiten aufdecken oder gar sensible Informationen über Krankheiten preisgeben könnte. Der den Einzelnen transparent, kalkulierbar und manipulierbar werden lässt für Dienste und Politik, Kommerz und Arbeitsmarkt“ … und eben auch Tatgelegenheit bietet für Kriminelle.

„Wir wollen und sollten die **Vorteile** der digitalen Welt **nutzen**, uns **gegen** ihre **Nachteile** aber **bestmöglich schützen**“, fordert der Bundespräsident. „Es gilt, Lösungen zu suchen, politische und gesellschaftliche, rechtliche, ethische und ganz praktische: Was darf, was muss ein freiheitlicher Staat im Geheimen tun, um seine Bürger durch Nachrichtendienste vor Gewalt und Terror zu schützen? Was aber darf er nicht tun, weil sonst die Freiheit der Sicherheit geopfert wird? Wie muss der Arbeitsmarkt aussehen, damit

1 *Münch*, Präsident des BKA, BKA Herbsttagung 2018, „Sicherheit in einer offenen und digitalen Gesellschaft, Begrüßungsrede, www.bka.de, 22.05.2020.

der allzeit verfügbare Mensch nicht zu so etwas wie einem digitalen Untertanen wird? Wie existieren Familie und Freundschaften neben den virtuellen Beziehungen? Wie können Kinder und Jugendliche das Netz nutzen, ohne darin gefangen zu werden? Wir brauchen also Gesetze, Konventionen und gesellschaftliche Verabredungen, die diesem epochalen Wandel Rechnung tragen."[2]

In diesem Spannungsfeld zwischen Freiheit und Sicherheit spiegeln die nachfolgenden aktuellen Schlagzeilen das Missbrauchspotenzial im Internet wieder![3]

Hacker-Bande ergaunert 1,65 Millionen Euro
NSA späht Kanzlerin-Handy aus
Gefahrenquelle Smartphone
Netzangriffe, Sabotage, Propaganda
Corona-Spam: Vorsicht vor falschen Masken-Mails
Radikalisierungsmaschinen – Wo Menschen zu Radikalen werden
Polizei zerschlägt Kinderporno-Ring – Haupttäter in Haft
Attacken auf Superrechner – Hacker greifen europaweit Hochleistungscomputer an
23-Jährige erstochen – Mörder im Netz kennengelernt
Wie aus Routern Zombies werden
Sicherheit im Netz hat ihren Preis

Seit 1997 erheben die großen deutschen Fernsehsender ARD und ZDF in einer repräsentativen Studie die Entwicklung der Internetnutzung in Deutschland. Danach nutzen rund 90 % der deutschsprachigen Bevölkerung ab 14 Jahren das Internet. Die deutlichsten Zuwächse gab es in 2019 bei der medialen Internetnutzung. Video-Streamingdienste wie Netflix gehören mittlerweile für 37 % zum wöchentlichen Medienrepertoire, aber auch Live-Fernsehen im Internet gewinnt an Beliebtheit. Audiostreaming über Spotify und Co. nutzen 13 % der Onliner, 20 % lesen mittlerweile online Artikel oder Berichte. Unter den Social-Media-Plattformen bleibt Facebook (21 % Tagesreichweite) Nummer Eins, Instagram ist der größte Gewinner (+4 %-Punkte auf 13 % Tagesreichweite). Die mediale Internetnutzung und Video-on-Demand gewinnen damit weiter an Bedeutung. Das Smartphone stellt bei der Internetnutzung unverändert ein ungemein rele-

2 *Gauck*, Bundespräsident, Rede zum Tag der Deutschen Einheit am 03.10.2013 in Stuttgart, www.bundespraesident.de

3 Aktuelle Schlagzeilen zur Berichterstattung diverser Tages- und Wochenzeitungen.

vantes Gerät dar und wird von der befragten Bevölkerung ab 14 Jahren zunehmend als Universalgerät eingesetzt.[4]

Die Reichweite des Internets ist damit vergleichbar mit der des Fernsehens. Das Internet zählt für die meisten Online-Nutzer zum Alltag und wird gewohnheitsmäßig täglich eingeschaltet.

Mit dem **Web 2.0 (Social Media)** entsteht seit 2003 eine „in sozio-technischer Hinsicht veränderte Nutzung des Internet, bei der dessen Möglichkeiten konsequent genutzt und weiterentwickelt werden. Es stellt eine Evolutionsstufe hinsichtlich des Angebots und der Nutzung des World Wide Web dar, bei der nicht mehr die reine Verbreitung von Informationen bzw. der Produktverkauf durch Webseitenbetreiber, sondern die Beteiligung der Nutzer am Web und die Generierung weiteren Zusatznutzens im Vordergrund stehen".[5]

Wikis, Blog, Microblogs, Social Networks und Social Sharing bezeichnen die Funktionsweisen der Kommunikation im Web 2.0.

Internetnutzer weltweit verbringen immer mehr Zeit mit sozialen Medien. Während die durchschnittliche Nutzungsdauer von sozialen Medien im Jahr 2012 noch bei 90 Minuten pro Tag lag, belief sich diese Nutzungsdauer im Jahr 2018 bereits auf 138 Minuten täglich. Gemessen an der durchschnittlichen Nutzungsdauer pro Tag ist unter 16- bis 19-Jährigen in Deutschland YouTube das beliebteste soziale Netzwerk. Die tägliche Nutzungsdauer belief sich im Durchschnitt auf 150 Minuten. Die zweithöchste Nutzungsdauer in dieser Altersgruppe erzielte Instagram mit 72 Minuten täglich. Unter den Deutschen ab 60 Jahren weist Facebook die höchste tägliche Nutzungsdauer auf.[6]

Smartphone, Tablets, Apps und die Cloud sind heute allgegenwärtig und gleichzeitig vielleicht auch schon wieder von gestern?! Neue Techniken sehen die Funktionen unserer ständigen Begleiter direkt in unseren Körper integriert (vgl. den Begriff Biohacking) – digitale Tattoos machen die Haut zum Medium, kleinste Chips unter der Haut mit kleinen Datenmengen, ins Ohr implantierte Bluetooth-Kopfhörer, operativ eingesetzte Elektroden zur Messung der Gehirnströme projizieren Gedanken in die Umgebung. Die Grenzen zum Cyborg[7] sind nicht mehr weit.

---

4 ARD/ZDF-Onlinestudie 2019, www.ard-zdf-onlinestudie.de, 19.05.2020.

5 *Gehl*, Kriminalität im Internet-Zeitalter, Vorwort zur Studientagung für Polizeibeamte, Richter, Staatsanwälte u. a., Katholische Akademie Trier 2012, zitiert aus http://wirtschaftslexikon.gabler.de, Stichwort: Web 2.0.

6 Statistiken zum Thema Soziale Netzwerke, https://de.statista.com, 19.05.2020.

7 Cyborg (von engl. „cybernetic organism") ein Lebewesen, das technisch ergänzt oder erweitert ist, https://wirtschaftslexikon.gabler.de, 19.05.2020.

Die Entwicklungen dauern an, im **Web 3.0**, dem sogenannte semantischen Web, kommt zu den nutzergenerierten Inhalten die Verknüpfung von Bedeutungen. Hier werden Informationen strukturiert und so aufbereitet, dass es Computern möglich ist, diese entsprechend ihrer Bedeutung zu verstehen und zu verarbeiten. Der Nutzer soll bei der Bewältigung der Informationsfülle unterstützt werden.

In Zukunft sollen nachfragebasierte Daten sowie intelligente Netzwerke die Nutzung des Webs dominieren. Ist von künstlicher Intelligenz die Rede, werden damit in aller Regel die IoT-Anwendungen des **Web 4.0** bezeichnet.[8]

Künstliche Intelligenz (KI) ist Innovationsmotor und Sicherheitsrisiko zugleich. KI gilt für immer mehr Bereiche als großer Zukunftstrend und wird schon heute in Unternehmen genutzt, um Abläufe zu automatisieren, Anwendungsprobleme zu lösen oder Sicherheitslücken aufzuspüren. Expertinnen und Experten gehen davon aus, dass KI schon bald in nahezu allen Unternehmensbereichen Einzug hält. KI wird aber auch eingesetzt, um Anomalien aufzudecken. Anomalien sind Abweichungen von bereits bekanntem Verhalten, und solche Abweichungen können auf bösartige Absichten hinweisen, die auf verärgerte Beschäftigte, Malware oder gar Kriminelle zurückgehen. Die Attacken sind in der Regel gut vorbereitet. Zuerst spionieren die Täterinnen und Täter mit Hilfe von Spionage-Software etwa E-Mails und Finanzdaten des Unternehmens aus, sichern sich Zugriff auf alle relevanten Systeme und installieren letztendlich die Verschlüsselungssoftware.[9]

Das Internet hat sich seit Beginn der 90er Jahre sprunghaft zum „Tummelplatz“ einer globalisierten Informations-, Wissensgesellschaft und Dienstleistungsgesellschaft entwickelt. Es dient als **uneingeschränkter Informationspool** und als **maßgebliches Kommunikationsmittel**. Der Kaufmann um die Ecke entwickelte sich zum Internethändler – der bequeme Einkauf von zuhause aus kann weltweit erfolgen. Mit dem Online-Service-Angebot wirbt die Wirtschaft: „Unnötige Wartezeiten am Telefon vermeiden, aktuelle Verträge einsehen, Angebotsberechnungen durchführen, Vertrags-, Adress- und Kontoänderungen vornehmen, Antworten auf Fragen zur Jahresrechnung finden.“ Die Furcht vor Viren und Ansteckung, Kontaktbeschränkungen und Abstandregeln fördern und verlangen die Internetnut-

8 Internet der Dinge (IdD), auch: „Allesnetz“, englisch Internet of Things, Kurzform: IoT, bezeichnet die Vernetzung von Gegenständen mit dem Internet, damit diese Gegenstände selbstständig kommunizieren können und dadurch Dienstleistungen absolvieren, https://wirtschaftslexikon.gabler.de, 19.05.2020.

9 Pressemeldung Zweites CyberSicherheitsForum, 19.02.2020, www.baden-wuerttemberg.de, 20.05.2020.

zung. Privates wird öffentlich, schon beim Telefonieren an jedem Ort mit dem Handy, jedenfalls beim uneingeschränkten Einsatz mobiler Computer auf Straßen und Plätzen und in öffentlichen Verkehrsmitteln oder durch die Eingabe und Nutzung persönlicher Informationen in sozialen Netzwerken.

Das Internet bestimmt so das Leben in vielen Bereichen und Situationen unseres Alltags.

Dabei hat die Technologisierung der Gesellschaft, wie bereits mehrfach angedeutet, auch ihre Schattenseiten, denn „Gelegenheit macht Diebe". Mit dem Internet entstand das sogenannte „global village". Dieses „globale Dorf" ist reich bevölkert. Jeder – mit Zugangsmöglichkeit, und es werden immer mehr – kann diesen Raum, dieses virtuelle neue Gebiet auch nutzen, um Straftaten zu begehen. Entsprechend bietet das Internet die **Plattform für neue Tatgelegenheiten und Kriminalitätsformen**. Auch Kriminelle nutzen die Vorzüge des Internets für ihre Zwecke aus. Digitale Beutezüge sind wesentlich lukrativer als herkömmlicher Betrug. Hinzu kommt das weit geringere Entdeckungsrisiko. Der „moderne Bankräuber" agiert im geschützten Raum am Computer, die **gefälschte IP-Adresse ersetzt die Maskierung**, **Gewaltanwendung** ist **nicht nötig** – ein **Mausklick genügt**.

Die rasante technologische Entwicklung beeinflusst die Erscheinungsformen von Kriminalität sowie Tat- und Tätertypologien nachhaltig, so BKA-Präsident Jörg Ziercke bei einer Konferenz mit dem Thema „Cybercrime – eine globale Gefahr?" bereits am 12.05.2010 in Kopenhagen.

Bei der Herbsttagung im Jahr 2013 warnte das BKA vor zunehmender Cyberkriminalität.[10] Der damalige Präsident des BKA, Jörg Ziercke, erkannte darin eine „Bedrohung mit unvergleichbarer Dimension. Die direkten Kosten, die durch Cybercrime entstehen, sind größer als jene, die der Handel von Kokain, Heroin und Marihuana gemeinsam erzeugen", sagte er in Wiesbaden.

Für Ziercke stand fest: „Durch die über das Internet zur Verfügung gestellte digitale Infrastruktur eröffnen sich neuartige Modi operandi mit enormen Schadensausmaß und -potenzialen." Das Internet entgrenze Kriminalität und sei ungebremst entwicklungsoffen. „Je mehr Geräte und Schnittstellen wir nutzen, je stärker wir uns digital vernetzen, desto mehr nimmt die Verwundbarkeit der Systeme zu."[11]

---

10 BKA-Herbsttagung am 12./13.11.2013 mit dem Thema „Cybercrime – Bedrohung, Intervention, Abwehr", Publikationen mit Tagungsprogramm und Rede- und Diskussionsbeiträgen finden sich unter www.bka.de

11 BKA warnt vor zunehmender Cyberkriminalität, http://www.tagesspiegel.de, Artikel vom 12.11.2013 zur BKA-Herbsttagung.

Eine vermeintliche Anonymität im Internet, die Erreichbarkeit großer Zielgruppen sowie deren teilweise fehlende Kompetenz im Umgang mit den neuen Medien begünstigen kriminelles Verhalten. In fast allen Kriminalitätsbereichen bedienen sich die Täter modernster Technik und nutzen das **Internet als Tatmittel**.

Es gibt kaum einen Computernutzer, der noch keinen Virus auf dem Rechner gehabt hätte. Geht der Angriff glimpflich ab, sind ein paar Daten verloren. In schlimmeren Fällen ist das Bankkonto geplündert oder die gesamte Identität ausgespäht. Für Wirtschaft und Verwaltung bedeutet Internetkriminalität mehr als persönlichen Ärger – sie bedroht öffentliche Infrastrukturen.

Hinter den Angriffen stehen auch oft kriminelle Netzwerke und Organisationen. Diese arbeiten hochprofessionell mit Hackern und Virenautoren über Staatengrenzen hinweg zusammen und verfügen über entsprechende Schadprogramme sowie die Infrastruktur zur Begehung von Straftaten im Internet. Das kriminelle Agieren ist durch eine besondere Dynamik gekennzeichnet, da sich die Täter veränderten technischen Gegebenheiten sehr schnell anpassen und enorme Innovationsfähigkeiten zeigen.[12]

Das sogenannte **Darknet**[13] bildet eine **digitale Parallelwelt** zum Internet, ein Netzwerk und globaler Marktplatz für Kriminelle, bezeichnet auch als **Underground Economy** – kriminelle wirtschaftliche Aktivitäten im Untergrund.

Ein spektakulärer Fall führt vor Augen, wie der Bankraub des 21. Jahrhunderts funktioniert: Innerhalb weniger Stunden hatten mehrere Internetbetrüger einer „New Yorker Zelle“ weltweit rund 45 Millionen Dollar an Bankautomaten abgehoben – ganz ohne Waffen und Sprengstoff. Der international agierenden Tätergruppierung war es gelungen, über kompromittierte Server in das Sicherheitssystem einer Bank einzudringen und sich die Kreditkartendaten zu verschaffen.[14]

Auf der Suche nach IT-Sicherheitslücken helfen „Werkzeugkisten“. Entsprechende Angebote sind auch bei Hackern gefragt. Sicherheitslücken aufzuspüren und darauf aufsetzende Angriffssoftware zu programmieren ist mühselig. Sammlungen, wie Metasploit oder Blackhole, helfen mit An-

12 Cyberkriminalität: Die globale Gefahr, in: Polizeispiegel 6/2010.ff, und *Münch*, Präsident des BKA, BKA Herbsttagung 2018, „Kriminalitätsbekämpfung weiterdenken – Phänomene – Herausforderungen – Handlungsoptionen im Zeitalter von Big Data, Algorithmen und autonomen Systemen“, dortige Fallskizze, www.bka.de, 20.05.2020.

13 Gleichbedeutend werden die Begriffe „Darkweb, „Deep Web“ verwendet.

14 Pressemeldung des IM Baden-Württemberg bzgl. „Internationales Symposium Cybercrime – Building Alliances for a Safer Digital World“, 17.10.2013.

griffsroutinen und Suchprogrammen, die auch versteckte Sicherheitslücken schnell finden. Auf der Website des Open-Source-Projekts www.metasploit.com tauschen sich Entwickler über sogenannte Penetrationssoftware, die Einbruchsstellen in Systeme ermittelt, und neueste Angriffsprogramme aus. Dort kann auch die „Metasploit Framework" genannte Werkzeugsammlung zur Entwicklung von Angriffssoftware heruntergeladen werden.

Während Systemadministratoren die **Software** einsetzen, um ihre Systeme auf Schwachstellen zu testen und gefundene Sicherheitslücken zu schließen, besteht so auch die **Möglichkeit** des **Missbrauch**s für Kriminelle. Die **Angriffsprogramme** eignen sich für nahezu alle kommerziell eingesetzten Betriebssysteme. Ein Exploit oder Angriffsprogramm dringt in ein Rechnersystem ein und installiert dort Schadsoftware (Spionageprogramme), stiehlt Kontendaten, vertrauliche Dokumente oder die Computeridentität der Anwender, löscht Festplatten, kidnappt das System oder manipuliert Steuerungsrechner von Industrieanlagen.

Blackhole ist eine Sammlung von Angriffsprogrammen, die laut dem Sicherheitsunternehmen Sophos bei einem Drittel aller Cyberattacken verwendet wird. Im Gegensatz zu Metasploit handelt es sich bei Blackhole um ein kommerzielles Produkt, das Jahresabonnement kostet 1.500 Dollar. Der Kunde erhält dafür nicht nur eine Sammlung von Angriffsprogrammen, sondern auch fortlaufende Lieferungen mit neu entdeckten, aber noch nicht bekannten Sicherheitslücken.[15]

Auch der Handel mit illegalen Waren und Dienstleistungen (Rauschgift, Waffen, digitale Identitäten, Kreditkartendaten, E-Mail-Accounts, Bankkonten [sogenannte „Bankdrops"][16], Anleitungen zu DDos-Attacken[17]) wird durch den Zugang zu entsprechenden Foren im Internet ermöglicht.

3D-Drucker ermöglichen die Herstellung funktionsfähiger Schusswaffen aus Kunststoffteilen, die so über das Internet illegal vertrieben werden können (vgl. Abb. 1).

15 *Welchenring*, Verschlungene Wege für mehr Sicherheit am Rechner, Frankfurter Allgemeine Sonntagszeitung, 14.04.2013.

16 *Burandt/Tölle*, Cybercrime – nicht nur in der Großstadt! – Erfahrungen am Beispiel einer Ermittlungskommission, in: Kriminalistik 8–9/2013.

17 Vgl. Kapitel 2.3, Cybercrime im engeren Sinn.