Berufsbegleitender Masterstudiengang
Informationsrecht (LL.M.)

Center für lebenslanges Lernen

PD Dr. Irini Vassilaki

Computer- und Internet-Strafrecht

Carl von Ossietzky Universität Oldenburg, 2017

Impressum

Autorin: PD Dr. Irini Vassilaki

Herausgeber: Universität Oldenburg, Center für lebenslanges Lernen C3L

Auflage: 11. Auflage, Erstausgabe 2007

Oldenburg, September 2017

INHALTSVERZEICHNIS

I. EINFÜHRUNG – KRIMINOLOGISCHE GRUNDLAGEN

Es gibt keine umfassenden wissenschaftlichen Untersuchungen, die belegen können, wie oft die neuen Medien für die Begehung von Straftaten missbraucht werden, welche Straftatbestände es gibt und wie häufig diese erfüllt werden oder wie hoch die Schäden aus dieser Kriminalitätsform sind.[1] Mehrfach fällt in diesem Zusammenhang das Stichwort „Kinderpornographie" oder „Volksverhetzung". Die Verbindung des Missbrauchs von neuen Telekommunikationsmedien mit der Verbreitung von pornographischen oder staatsgefährdenden Inhalten würde dieser Kriminalitätsform nicht gerecht, denn ein oberflächliches Durchblättern der strafrechtlichen Entscheidungen, die sich mit dieser Frage beschäftigen, weist schon darauf hin, dass die „multimediale Kriminalität"[2] oder die „Internet- oder „Post-Computerkriminalität"[3] viele Erscheinungsformen hat. Es trifft wohl zu, dass keine sicheren Angaben hinsichtlich der Erscheinungsformen der multimedialen Kriminalität gemacht werden können, weil einschlägige kriminologische Analysen fehlen.[4]

Das Bundeskriminalamt (BKA) hat für 2010 mehr Straftaten im Bereich der Computerkriminalität festgestellt. Besonders beim Ausspähen und Abfangen von Daten ist ein Anstieg der Straftaten aufgefallen. Bei den Straftaten, bei denen das Internet als Tatmittel eingesetzt wird, handelt es sich der polizeilichen Kriminalstatistik zufolge hauptsächlich um Waren- und Warenkreditbetrug. Der Betrug mit Zahlungskarten, bei denen die Täter die Daten nicht rechtmäßig erworben haben, hat um 11,9 Prozentpunkte zugenommen. Insgesamt handelt es sich deutschlandweit im Jahr 2010 um 19.100 Fälle.

In 15 Bundesländern (eines wurde wegen 2009 fehlender Daten nicht mitgerechnet) wurden 2010 insgesamt 223.642 Straftaten erfasst, die über das Internet begangen wurden. Gegenüber 2009 ist dieser Wert um 8,1 Prozentpunkte angestiegen, in absoluten Zahlen ist das bislang der höchste Wert. Zu 81,6 % handelt es sich dabei um Betrugsdelikte. Auch die Zahl der Fälle von Computerbetrug ist gestiegen, um 8,0 Prozentpunkte. Einen auffälligen Anstieg verzeichnen die Statistiker der Polizei beim Ausspähen und Abfangen von Daten. Hier hat sich die Zahl der Delikte von 3,3 % auf 4,2 % erhöht. Die Computerkriminalität insgesamt stieg 2010 um 12,6 Prozentpunkte auf 84.377 Fälle. Die Behörden berich-

---

1 S. auch *Gercke*, ZUM 2010, S. 638.

2 Zu diesem Begriff *Vassilaki*, CR 1997, S. 297; dazu auch *Barton*, Multimedia Strafrecht, 1999, S. 34; *Bremer*, Strafbare Internet-Inhalte in internationaler Hinsicht, 2001, S. 61; *Dornsreif/Schumann/Klein, DuD 2002, S. 226*.

3 Vgl. dazu *Vassilaki,* MMR 2006, S. 212.

4 S. dazu *Shimada,* CR 2009, S. 689, der für die Bestrafung der Internetkriminalität die Notwendigkeit der „Vorfeldkriminalisierung" heranzieht.

ten, dass Betrug, Kinderpornographie und sexueller Missbrauch immer stärker in Zusammenhang mit neuen Informationstechnologien stünden.

Über alle Straftaten gesehen ist die Zahl der Fälle seit 1993 um 12,1 % zurückgegangen. Die Aufklärungsquote erhöhte sich in diesem Zeitraum von 43,8 auf 56 %. Im Bereich der Computerkriminalität dagegen konnte die Polizei weniger Delikte aufklären: Bei der Computersabotage sank die Aufklärungsquote um 4,8 Prozentpunkte, beim Betrug mit Internet- und Kommunikationsmitteln um 2,2 Prozentpunkte.[5]

Im Jahr 2011 ist das Bild gemischt. Nachdem 2010 Großverfahren im Zusammenhang mit Online-Auktionsplattformen abgeschlossen worden waren, ging der Warenbetrug im Internet 2011 deutlich zurück. Ohne Berücksichtigung des Warenbetrugs wäre die Internetkriminalität um fünf Prozent auf 15.425 Fälle gestiegen. Die digitale Schutzgelderpressung explodierte von zwei auf 2.899 Fälle. Besitz und Verschaffen von Kinderpornografie im Internet ist um ein Sechstel auf 327 Straftaten angewachsen.[6]

Die Bedrohung durch Cyberkriminalität in Deutschland nimmt laut einem Lagebericht des Bundeskriminalamts (www.bka.de) trotz stagnierender Fallzahlen weiter zu. Im Jahr 2011 hat es rund 60.000 Fälle von Internet-Kriminalität gegeben. Der verursachte Schaden ist um 16 % auf schätzungsweise 71,2 Millionen Euro gestiegen. Die größte Straftatengruppe sei dabei der Computerbetrug gewesen: Mit Phishing-Mails und dem missbräuchlichen Einsatz von Kreditkartendaten ist ein Schaden von rund 50 Millionen Euro entstanden. Obwohl die kriminellen Aktivitäten zugenommen haben, ist die Dunkelziffer sehr hoch. Für die Verbreitung von Schadsoftware wurden vermehrt Botnetze genutzt. Das Phishing von Onlinebanking-Daten oder der missbräuchliche Einsatz von Kreditkartendaten machen mit 45 % die mit Abstand größte Gruppe der Bedrohung aus. Ein zunehmend attraktives Ziel ist auch das Smartphone. Unternehmen sind von den Cyberattacken ebenso betroffen wie Privatnutzer. 40 % der Unternehmen in Deutschland verzeichneten teils mehrmals Angriffe auf ihre IT-Systeme. Ein Drittel hat demnach bereits Erfahrungen mit dem Verlust von Daten gemacht.[7]

Im Jahr 2012 sind – laut der polizeilichen Kriminalstatistik 2012 – die in Deutschland im Internet erfassten Delikte sowie Straftaten mit Computerbezug im Vergleich zum Vorjahr um jeweils gut 3 % angestiegen. Strafverfolger registrierten 229.408 Fälle von Kriminalität „unter Nutzung des Tatmittels Internet“, wozu vor allem Betrugsdelikte zählen. 2011 waren es noch 222.267. Der Bereich Computerkriminalität umfasste 87.871 Vergehen statt 84.981 im Vorjahr. Straftaten, bei denen Täter moderne Informations- und Kommunikationstechnik (IuK) ausnutzen, indem sie etwa Daten ausspähen und abfangen, mit einer Schadsoftware Informationen verändern oder Systeme beschädigen, sind 2012 im Vergleich zu 2011 um 7,5 % auf 63.959 Fälle nach oben geschnellt. Besonders hoch ist die Zunahme um

5 PKS 2010, S. 5.

6 S. Polizeiliche Kriminalstatistik 2011.

7 BKA, Cybercrime, 2011, S. 6, 18.

rund 130 % bei Computersabotage etwa mit DDoS-Attacken und Datenveränderung von 4.644 auf 10.857 Straftaten. Der Betrug mit Zugangsberechtigungen zu Kommunikationsdiensten ging in diesem Sektor dagegen am stärksten um fast 38 % auf 2.952 Fälle zurück. Die Aufklärungsquote bei Cybercrime ist um 3,5 Prozentpunkte auf 26,5 % und im Teilbereich Datenmanipulation und Sabotage massiv um 23,7 Prozentpunkte auf 17,5 % zurückgegangen. Die Polizei geht bei Cyber- sowie Computerkriminalität insgesamt von einem „erheblichen Dunkelfeld" aus. In die Statistik gingen nur Taten ein, bei denen der Verdächtige in Deutschland am Computer sitzt. In vielen Fällen nutzten Kriminelle aber Server im Ausland und starteten ihre Angriffe auch von dort aus. Wie im Vorjahr nahm 2012 die Verbreitung pornographischer Schriften ab, und zwar um 11,6 % auf 7709 Fälle. Ein Teilbereich davon ist der Besitz und die Verschaffung von Kinderpornographie, der ebenfalls weiter rückläufig ist: Er sank um 16,9 % auf 3239 in die Statistik eingegangene Delikte. Die Aufklärungsquote ist hier um 1,2 Prozentpunkte angestiegen. Eine leichte Steigerung um 89 auf 2.465 Fälle ist dagegen bei der Verbreitung von Inhalten rund um sexuellen Kindesmissbrauch festzustellen, während die Aufklärungsquote bei diesen Straftaten niedriger als im Vorjahr (67,7 statt 72,8 %) war. Vergehen im Zusammenhang mit Urheberrechtsbestimmungen wiesen im Gegensatz zu 2011 wieder einen Anstieg um 5,6 % auf 7.417 Fälle auf. Insgesamt zählt die Statistik – wie in den beiden Jahren zuvor – weniger als 6 Millionen Vergehen. Gegenüber dem Vorjahr wuchs ihre Zahl geringfügig um 0,1 % auf 5.997.040 Straftaten an. Die Aufklärungsquote lag fast unverändert bei 54,4 % im Vergleich zu 54,7 % 2011. Die Zahl der Tatverdächtigen reduzierte sich um 0,9 % auf rund 2,10 Millionen Personen.[8]

Auch das Landeskriminalamt von Mecklenburg-Vorpommern erwartet eine weitere Zunahme von Straftaten mit Hilfe des Internets. Bereits für 2011 gab es in dem Bundesland einen Anstieg von 9,3 % der Internetstraftaten auf 5.304 Fälle. Schwerpunkt der Cyberkriminalität ist der Betrug beim Kauf und Verkauf von Waren. Aber auch Angriffe auf private Computer oder Behördenrechner mit Schadsoftware sowie das Ausspähen sensibler Daten und Sabotage nähmen zu. Selbst bei Polizeibehörden und dem Landeskriminalamt hätte es schon Hackerattacken gegeben.[9]

Laut einer Studie von Hewlett-Packard verursachen Datendiebstahl, Computerviren und Web-Attacken in einem deutschen Großunternehmen jährlich einen Schaden von durchschnittlich 4,8 Millionen Euro. Deutschland liegt in der Statistik damit zwischen den USA (6,9 Millionen Euro) und Japan (3,9 Millionen Euro). Pro Woche gibt es in den für die Studie untersuchten Unternehmen und Behörden 1,1 erfolgreiche Angriffe – verglichen mit 1,8 in den USA. Allein 40 % des geschätzten Schadens entfallen auf Datenverluste – oft verursacht durch „Taten

8 Polizeiliche Kriminalstatistik 2012, S. 5.

9 www.heise.de/-1775338.

krimineller Insider“. Weitere 28 % fallen als Umsatzeinbußen an, etwa wenn nach einer Denial-of-Service-Attacke die Shopping-Webseite lahmgelegt wird.[10]

International belegt eine neue Studie der Sicherheitsfirma Symantec, dass Privatpersonen weltweit rund 110 Milliarden US-Dollar (derzeit rund 88 Milliarden Euro) an finanziellen Schäden durch Cyberkriminalität erlitten haben. In dem erfassten Zeitraum von Juli 2011 bis Juli 2012 soll jedes Opfer im Schnitt 197 US-Dollar (rund 157 Euro) eingebüßt haben. Neuer Trend scheint der Missbrauch Sozialer Netzwerke und mobiler Geräte zu sein: 20 % derer User wurden zum Opfer. Bei 15 % wurde – laut Studie – der Social-Media-Account gekapert und 10 % fielen auf falsche Links und Spam über soziale Netzwerke rein. Insgesamt glauben 75 % der Befragten, dass die Cyberkriminellen immer stärker in sozialen Netzwerken aktiv werden.[11]

Nach einer GfK-Studie ist fast jeder zweite Surfer (47,6 %) schon einmal Opfer von Internetkriminalität geworden. Am häufigsten haben Betroffene mit Schadsoftware auf ihrem Rechner zu kämpfen (25,7 %) oder fallen beim Online-Einkauf und bei Internet-Diensten Betrügern zum Opfern (16,8 %). Viele Nutzer berichten über unbefugten Zugriff auf ihre persönlichen Daten sowie deren Missbrauch oder Diebstahl (10,9 %). Auch vermeintlich kostenlose Dienstleistungen, für die später doch gezahlt werden muss, sind der Umfrage zufolge ein größeres Problem (10,8 %). Für die Studie zum Safer Internet Day am 5. Februar waren insgesamt 1.000 Internetnutzer repräsentativ befragt worden.[12]

Laut der Polizeilichen Kriminalstatistik (PKS) 2013 haben die Ermittlungsbehörden 64.426 Fälle und damit gegenüber dem Vorjahr einen Anstieg um 0,7 % registriert. Im Teilbereich der Computersabotage und Datenveränderung schnellten die erfassten Fälle um 17,6 % auf 12.766 nach oben. Diese Zunahme wird vor allem durch häufigere Angriffe durch Schadsoftware wie Trojaner erklärt. Zugleich sank die Aufklärungsquote in diesem Sektor von 17,5 auf 9,2 %. Der erfasste Computerbetrug ist allerdings um 6,3 % auf 23.242 Fälle zurückgegangen, die Aufklärungsquote hier sogar leicht auf 31,1 % gestiegen. Ein Minus von 7,5 % bei 2.730 registrierten Taten weist die PKS beim Erschleichen von Zugangsberechtigungen zu Kommunikationsdiensten aus, bei einer deutlich auf 42,6 % nach oben gekletterten Quote der Ermittlungserfolge. Auch beim Ausspähen und Abfangen von Daten hat die Polizei weniger Straftaten erfasst: 15.909 im Vergleich zu 16.794 im Jahr zuvor. Die Aufklärungsquote liegt hier mit 18,3 % etwas höher. Eine um 14,5 % zunehmende Tendenz ist dagegen bei der Fälschung beweiserheblicher Informationen und der Täuschung im Rechtsverkehr bei der Datenverarbeitung mit 9.779 Fällen festzustellen. Der übergeordnete Bereich der gesamten Computerkriminalität ist um 1 % auf 88.722 erfasste Delikte angestiegen. Die Aufklärungsquote ist dabei leicht um 1,1 auf 28,8 % zurückgegangen. Insgesamt wurden zudem 257.486 Fälle erfasst, die mithilfe des „Tatmittels In-

10 3rd Annual Cost of Cyber Crime Study, 2012.

11 S. 2012 Cybercrime Report.

12 http://www.e-commerce-blog.de/2013/02/08/internetkriminalitat-eine-prasente-gefahr/8670/.

ternet“ begangen wurden, was einem Plus von 12,2 % gleichkommt. Überwiegend handelte es sich dabei um Betrugsdelikte wie eine Online-Bestellung von Waren, für die nach Lieferung nicht gezahlt wird. Die 6.597 Fälle pornografischer Schriften, die über das Internet verbreitet worden sind, machen 31,1 % mehr als 2012 aus. Dieser Tatbereich macht 2,6 % aller online begangenen Delikte aus. Die Aufklärungsquote ist in diesem Sektor um 3,8 Punkte angestiegen, rangiert nun bei 84,8 %. Ein Teilbereich ist der Besitz und die Verschaffung von Kinderpornografie mit ebenfalls ansteigender Tendenz: plus 27,9 % auf 4.144 Fälle. Die seit dem Jahr 2009 zunehmende Zahl der Straftaten des sexuellen Kindesmissbrauchs ist im aktuellen Berichtsjahr erstmals wieder um 1,5 % leicht rückläufig auf 12.437 Vorgänge. Generell hat die Polizei wie bereits in den beiden Vorjahren auch 2013 weniger als sechs Millionen Delikte registriert, nämlich genau 5.961.662. Die Aufklärungsquote liegt mit einem Wert von 54,5 % ganz leicht über dem Niveau von 2012. Die Zahl der Tatverdächtigen ist mit etwas über zwei Millionen gegenüber dem Vorjahr konstant geblieben.[13]

Die Anzahl der auf Cybercrime entfallenden Straftaten ist laut PKS 2014 für das Jahr 2014 gegenüber den Vorjahren im Bundesdurchschnitt deutlich geringer, zugleich sind die Aufklärungsquoten gestiegen. Diese Zahlen sind mit der Tatsache verbunden, dass die PKS für das Jahr 2014 nur solche Straftaten erfasst hat, für die konkrete Anhaltspunkte vorliegen, dass die Tathandlung in Deutschland durchgeführt wurde. Auf dieser Grundlage wurden für 2014 49.925 Fälle registriert. Die Aufklärungsquote betrugt 29,3 % und im Teilbereich „Datenveränderung und Computersabotage“ 17,7 % (2013: 9,2 %). Insgesamt wurden im Jahr 2014 73.900 Fälle von „Computerkriminalität“ registriert, darunter 11.887 Fälle von „Ausspähen und Abfangen von Daten einschließlich Vorbereitungshandlungen“ sowie 5.661 Fälle von „Datenveränderung und Computersabotage“.[14]

Nach einer Bitkom-Umfrage seien 55 % der Befragten im Jahr 2013 Opfer von Cybercrime geworden. Hochgerechnet wären dies also 29 Millionen Bundesbürger, die unter Cybercrime-Attacken gelitten hätten. Bei 40 % der Befragten sei der Computer mit Schadprogrammen infiziert worden. 47 % der Befragten verschicken vertrauliche Texte nicht mehr per Internet-Mail, 16 % der Befragten verschlüsseln die Emails. Im Vorjahr waren dies nur 6 %. Schwächer fiel der Anstieg bei der Nutzung von Anonymisierungsdiensten wie Tor aus; er stieg von 11 auf 16 %.[15]

Mithin ist das Gefährdungs- und Schadenspotenzial des Phänomens Cybercrime unverändert hoch.[16]

Die Zahl der Computer- und Cybercrimestraftaten ist laut Polizeikriminalitätstatistik im Jahr 2015 gegenüber dem Jahr 2014 um 8,3 % zurückgegangen. Die Aufklä-

---

13 Siehe Polizeiliche Kriminalstatistik 2013, S. 11, 81, Cybercrime Bundeslagebild 2013.

14 PKS 2014, S. 6, 12, 13.

15 Siehe dazuhttp://www.bka.de/DE/Presse/Pressemitteilungen/Presse2014/140827__BundeslagebildCybercrime.html?__nnn=true

16 BKA, Cybercrime 2010, Bundeslagebild 2010, S. 14.

rungsquote lag bei 32,8 %. Die Computerbetrugsfälle haben um 5,6 % zugenommen und bilden damit die Mehrheit der Cybercrimestraftaten. Die Schadenssumme in diesem Bereich betrug 40,5 Mio. Euro. Dies entspricht einer Zunahme um 2,8 % gegenüber dem Vorjahr. Dies bedeutet, dass es im Jahr 2015 weniger Fälle der Cyberkriminalität allerdings mit steigender Qualität gab.[17] Schadsoftware wurde im Jahr 2015 als häufigste Angriffsart benannt.[18]

Um den neuen Gefahren entgegenzutreten, haben sich der EU-Rat und das Europäische Parlament Anfang Dezember 2015 auf neue IT-Sicherheitsregeln verständigt. Diese Regeln gewährleisten eine hohe gemeinsame Netz- und Informationssicherheit insbesondere im Bereich wichtiger Infrastrukturen. Die Mitgliedsstaaten sollen nationale Meldesysteme einrichten und Informationen untereinander austauschen, während Betreiber von kritischen Infrastrukturen und größerer Online-Dienste in die Pflicht genommen werden, ihre IT-Systeme sicherer zu machen und Angriffe sowie andere Sicherheits- und Datenschutzpannen zu melden.[19]

Nach einer Studie von ENISA erreicht der Schaden von Angriffen auf kritische Informationsinfrastrukturen in einigen EU-Ländern 1,6 % des Bruttoinlandsozialprodukts.[20]

Nach einer KPMG-Studie zum „e-crime“ lagen die Schäden der 504 befragten Unternehmen von 2014 bis 2016 je Unternehmen in der Regel zwischen wenigen Zehntausend Euro bis mehreren Hunderttausend Euro. In einigen Fällen ging die Gesamtschadenssumme deutlich darüber hinaus. Drei Viertel der Befragten nannten Schäden im Bereich bis zu 250.000 Euro. Die Hälfte der Angaben bewegte sich im Bereich zwischen 15.000 und 120.000 Euro. Jedes zwanzigste Unternehmen gab jedoch mehr als eine Million Euro an Schäden an, bei größeren Unternehmen sogar jedes zehnte. Die höchsten Schäden wurden für die Delikte „Verletzung von Geschäfts- oder Betriebsgeheimnissen“ und „Verletzung von Urheberrechten“ genannt. „Datendiebstahl“ und „Manipulation von Konto- und Finanzdaten“ waren die häufigsten Delikte, auf die die höchsten Schadenssummen entfielen. Drei Viertel der Schadenssummen bewegten sich im Bereich bis 100.000 Euro.[21]

Nach einer PWC-Studie wurde „Cyber-crime“ im Jahr 2016 zum zweithäufigsten berichteten Erscheinungsphänomen der Wirtschaftskriminalität. 50 von den befragten Unternehmen gaben an, dass sie Schäden über $ 5 Mio. erlitten haben. In dieser Studie wurden als häufigste gemeldete Delikte der Cyberbetrug und der IP-Angriff genannt.[22] Nach der Polizeilichen Kriminalstatistik des BKA wurden im

---

17 Siehe Cybercrime, Bundeslagebericht 2015, S. 4

18 https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Micro/Umfrage/umfrage2015.htm.

19 http://www.europarl.europa.eu/news/en/news-room/20151207IPR06449/meps-close-deal-with-council-on-first-ever-eu-rules-on-cybersecurityF.

20 The cost of incidents affecting CIIs, S. 4.

21 *KPMG*, e-crime, S. 9.

22 *PWC,* Adjusting the Lens on Economic Crime, S. 18, 19.

Jahr 2016 107.751 Fälle von Computerkriminalität registriert. Ihr Anteil an der Gesamtkriminalität beträgt 1,7 %/1,8 %. Den größten Teil davon bilden Fälle des Computerbetrugs (84.060 Fälle). Danach folgen Fälle von Datenspionage (Ausspähen, Abfangen von Daten: 10.638 Fälle). Die Tatverdächtigen sind überwiegend deutsche männliche Erwachsene ab 21 Jahren.[23]

Aus einer Studie der Bitkom ergibt sich, dass mehr als jedes zweite Unternehmen in den Jahren 2015 bis 2017 aus dem Internet angegriffen worden ist, 53 Prozent der deutschen Firmen wurden Opfer von Wirtschaftsspionage, Sabotage oder Datendiebstahl. Der Schaden der Angriffe beträgt die Summe vom 55 Milliarden Euro jährlich, Allerdings nicht einmal jede dritte betroffene Firma (31 Prozent) zeigt die Vorkommnisse den Behörden an. Von denen meldet nur jedes siebte Opfer die Vorgänge der Datenschutzaufsicht oder dem Bundesamt für Sicherheit in der Informationstechnik. Hauptgrund für die mangelnde Meldemoral ist die Angst vor Imageschäden (41 Prozent). Andere gaben an, sie hätten darauf verzichtet, weil sie Angst vor negativen Konsequenzen hätten oder annähmen, dass die Täter sowieso nicht gefasst würden oder der Aufwand zu hoch sei. Die Täter kommen in der Mehrzahl der Fälle aus der aktuellen und früheren Belegschaft, während in einer Mehrheit der Fälle die Spur ins Ausland vor allem nach Osteuropa (23 Prozent), China (20), Russland (18) und in die USA (15) führt.[24]

Aus sowohl durch die Presse und aus Studien bekannt gewordenen als auch aus von Strafgerichten judizierten Fällen lassen sich folgende Kategorien bilden, die den Missbrauch der neuen Telekommunikationsmedien betreffen:

- Wirtschaftsdelikte,
- Delikte gegen den demokratischen Rechtsstaat,
- Delikte gegen die Persönlichkeit i.w.S.,
- Delikte gegen die Jugend i.w.S.

1. Wirtschaftsdelikte

Dass die neuen Informationstechnologien für den Abschluss und die Durchführung von Geschäften verwendet werden, ist eine Binsenwahrheit. Aus diesem Grund liegt es nahe, dass E-Commerce ein beliebtes Betätigungsfeld für Kriminelle darstellt. In diesem Zusammenhang erfasst diese Kategorie der multimedialen Kriminalität jede Tätigkeit, die die Erscheinungsformen des E-Commerce missbraucht, um finanzielle Vorteile für den Täter zu erlangen. Die Manipulationen, die im Zuge des Ablaufs etwa von Online-Auktionen durchgeführt werden, die strafbaren urheberrechtlichen Verletzungen bei der Online Übermittlung etwa von Software oder Musik oder die Verletzung von Geschäftsgeheimnissen

---

23 *PKS,* Berischtsjahr 2016 S. 166-171.

24 *Bitkom,* Wirtschaftsschutz in der digitalen Welt, S. 2, 5-7, 9.

während der Online-Nutzung einer Datenbank, stellen nur ein paar Beispiele dar, die den wirtschaftlichen Teil des Medienstrafrechts bilden.

Insbesondere fördert der unkörperliche Kontext des „Cyberraums" die Verletzung des geistigen Eigentums. Im Jahr 2010 wurden in Deutschland Programme im Wert von rund 1,6 Milliarden Euro raubkopiert. 27 % aller verwendeten Programme sind illegal. In der EU stagniert der Anteil unlizenzierter Software bei 35 %. Der Wert stieg allerdings von 8,3 auf umgerechnet 10,1 Milliarden Euro. Was das Volumen der Raubkopien angeht, liegen weltweit die USA (20 %, 9,5 Milliarden US-Dollar), China (78 %, 7,8 Milliarden US-Dollar) und Russland (65 %, 2,8 Milliarden US-Dollar) an der Spitze.[25] Nach der „Brennerstudie 2010" geht die Zahl der illegalen Musikdownloads zurück. Die Zahl der illegalen Musikdownloads sank von 316 Millionen in 2008 auf 258 Millionen in 2009. Der typische Filesharer ist männlich und 20-39 Jahre alt. Von den rund 4,5 Millionen Deutschen, die sich illegal mit Musik, Filmen, Games oder (Hör-)Büchern aus dem Internet versorgen, sind in der Altersgruppe der 20- bis 29-jährigen Männer mit 25 % und bei den 30- bis 39-jährigen Männern mit 17 % die meisten Filesharer zu finden. Dies zeigt, dass es sich bei Tauschbörsennutzern nicht überwiegend um Kinder und Jugendliche handelt. Nach den Zahlen nutzte unter den 10- bis 19-Jährigen nicht mal jeder zehnte Jugendliche (9 %) die illegalen Angebote.[26]

Die AfD-Studie „Online-Filmpiraterie transparent gemacht" hebt hervor, dass 65 % aller Filme als Raubkopien in den Tauschbörsen erscheinen. Davon taucht 1/3 schon vor dem Kinostart oder am Startwochenende im Internet auf, während 45 % in den ersten beiden Wochen nach der Premiere im Internet verfügbar ist. Der Online-Anteil der Filmpiraterie in den Vereinigten Staaten und Großbritannien ist hoch. In Deutschland liegt er im Mittelfeld.[27]

Ende August 2014 hat ein Gericht im englischen Wolverhampton einen 25-Jährigen zu 33 Monaten Gefängnis verurteilt, der Filme illegal aufgezeichnet, im Netz verbreitet und verkauft hatte. Sein Mitangeklagter wurde zu 120 Sozialstunden verurteilt. Der Hauptangeklagte hatte im Mai 2013 eine Kinovorstellung des US-Films „Fast and Furious 6" mit einem Camcorder abgefilmt und im Netz verbreitet. Nach Angaben der britischen Federation Against Copyright Theft (FACT) war das die erste illegale Kopie des Streifens im Netz und wurde rund 700.000 Mal heruntergeladen. FACT beziffert den dem Filmstudio und der britischen Branche entstandenen Schaden auf „mehrere Millionen Pfund". Laut FACT wirkte strafverschärfend, dass der Verurteilte den Streifen nicht nur gratis im Netz verbreitet hat, sondern Kopien auch von anderen Filmen wie „Iron Man 3" für 1,50 Pfund (1,90 Euro) über Facebook verkauft hat. Zudem soll Philip D. weiter Filme illegal verbreitet haben, auch nachdem er festgenommen und vernommen worden war.[28]

---

25 S. Eighth Annual BSA Global Piracy Study (2010).

26 Siehe die Ergebnisse der Brennerstudie 2010.

27 AfD-Studie, Online-Filmpiraterie transparent gemacht, 2005, S. 4 (5).

28 Siehe dazu http://www.fact-uk.org.uk/cammer-sentenced-to-33-months-imprisionment/.

Gleichwohl weist eine Umfrage des Instituts American Assembly der Columbia University im Rahmen der Studie „Copy Culture in the US and Germany" darauf hin, dass US-amerikanische Erwachsene, die an Tauschbörsen teilnehmen, durchschnittlich eine größere Sammlung an digitalen Musiktiteln besitzen als jene, die kein Filesharing betreiben. Dieses Ergebnis klingt nicht überraschend. Die Tauschbörsenteilnehmer geben auch mehr Geld für Musikstücke aus als die Nicht-P2P-Nutzer.[29]

Der Bundesverband der Musikindustrie (BVMI) hat gemeldet, dass im Jahr 2012 die legalen Downloads um 22,4% gestiegen sind. Von den knapp 115 Millionen Downloads entfallen 97 Millionen auf einzelne Tracks (+22,9 %), 16 Millionen und damit 55 % aller Downloadumsätze auf komplette Alben (+20,6 %) und 1,5 Millionen auf Single-Bundles (+12,8 %).[30]

Wie eine Studie, die die Firma McAfee in Auftrag gegeben hat, darlegt, werden die Informationstechnologien von organisierten Kriminellen angewendet, um Gewinne aus Straftaten, etwa durch Betrug, Erpressung und Kindesmissbrauch zu erzielen. Dafür werden professionelle Hacker oder Viren-Programmierer angeheuert, die auf Bestellung Eingriffe gegen Netzwerke vorbereiten und durchführen.[31] „Hacking" ist bereits seit den achtziger Jahren eine bekannte Form der Computerkriminalität. Die Attacken auf Informationssysteme haben in den letzten zehn Jahren einen anderen Charakter angenommen. Das Motiv der Täter ist nicht – wie in den 80er Jahren – nur in der Herausforderung zu suchen, technische Systeme zu knacken. Bei den meisten Angreifern handelt es sich nun um Hacker, die bezahlt werden, um die Sicherheitsmaßnahmen von Computernetzen zu überwinden, Daten zu manipulieren oder Netzwerke zu beschädigen. Angreifer dringen in großer Zahl in Netzwerke ein und verursachen absichtlich Schäden in Millionenhöhe. Bezeichnend für diese Entwicklung ist der sog. „Liquid FX-Fall". Im März 2004 haben 15 Polizeigruppen 132 Wohnungen von Mitgliedern des Hackerforums "Liquid FX" durchsucht. Die Ermittlungen, die zur Anklage von 126 Hackern führten, ergaben, dass es sich bei „Liquid FX" um eine grenzüberschreitende Organisation handelte, der 476 Mitglieder aus 33 Ländern angehörten. Sie betrieben 11.820 „Zombies"[32] in 83 Ländern, von denen 619 in Deutschland festgestellt worden waren. Sie wurden verwendet, um Raubkopien von Software, Musik und Filmdateien zu speichern.[33]

Aus diesem Hackerprofil soll der „Hackeraktivist" differenziert werden. Dieser ist ein Hacker, dessen Ausübung von Taten nicht-profitorientiert und ideologisch motiviert und auf Zwecke des Protests und der Propaganda aus ist. Außerdem wird der Ha-

---

29 Copy Culture in the US and Germany, S. 47.

30 http://www.musikindustrie.de/presse_aktuell_einzel/back/82/news/mehr-als-100-millionen-legale-musikdownloads-in-2012/

31 Siehe dazu Bericht von McAfee zum Thema virtuelle Kriminalität, Februar 2005, S. 6.; auch Vassilaki, MMR 9/2003, S. V.

32 Zombies sind infizierte Computer, die sich unter der Kontrolle einer anderen Person als des rechtmäßigen Nutzers befinden.

33 So der Bericht von McAfee zum Thema virtuelle Kriminalität, S. 8.

ckeraktivismus überwiegend von Gruppierungen ausgeübt. Der Hackeraktivist ist – einer BKA-Untersuchung zufolge – in 90 % der Fälle männlichen Geschlechts und zwischen 18 und 30 Jahren alt.[34]

Mit einem virusähnlichen Programm bemächtigten sich Hacker im Juni 2005 in den USA der Daten von über 40 Mio. Kreditkarteninhabern. Die Täter drangen in das Computersystem einer Firma ein, die Transaktionen zwischen Konsumenten, Handel und Kreditkartenfirmen abwickelt. Das Unternehmen VISA teilte mit, dass bei ca. 40.000 dieser Karten die Inhalte der Magnetstreifen entwendet wurden, so dass größte Betrugsgefahr bestand.[35]

Schadsoftware wurde über Terminals in den Ladengeschäften der Firma „Neiman Marcus" eingeschleust, und vom 16. Juli bis 30. Oktober 2013 sammelte diese Kartendaten. Die Software hätte dabei auf 1,1 Millionen Datensätze zugreifen können. Visa, MasterCard und Discover hätten bislang von 2.400 Missbrauchsfällen berichtet, die mit dem Datendiebstahl in Verbindung stünden.[36]

Im April 2013 haben durch den Einsatz eines sog. Carberp-Trojaners Kriminelle aus der Ukraine und Russland rund acht Milliarden russische Rubel und drei Millionen ukrainische Griwna erbeutet – umgerechnet etwa 200 Millionen Euro. Die betroffene Sberbank meldete, dass die Kriminellen Trojaner der Carberp-Familie anwendeten, weiterentwickelten und -verkauften. Anführer der Bande war ein 28-jähriger Russe aus der ukrainischen Schwarzmeerstadt Odessa. Den Hackern drohen jeweils bis zu sechs Jahre Haft. Erst vor einigen Wochen wurde eine Gruppe von Kriminellen in Russland verhaftet, die mit dem Carberp-Trojaner etwa 3 Millionen Euro erbeutet haben sollen. Ob die kriminellen Gruppen und deren Festnahmen miteinander in Verbindung stehen, ist unklar.[37]

Im Oktober 2012 haben Hacker durch DDoS-Attacken die Internet-Auftritte schwedischer Behörden und Banken zeitweise lahmgelegt, u.a. die von Schwedens Zentralbank, des Reichstages, des Polizeigeheimdienstes Säpo, der Staatsanwaltschaft und anderer Behörden. In einem Youtube-Clip im Namen der Hacker-Bewegung Anonymous wurde die großangelegte Aktion angekündigt. Als Begründung wurde dabei unter anderem die Razzia gegen den Webhoster PeRiQuito (PRQ) angegeben, die die schwedische Polizei durchführte. PRQ stellt unter anderem Server für Torrent-Dienste zur Verfügung und war bis vermutlich 2010 auch der Hoster der Whistleblower-Plattform Wikileaks. Diese Polizei-Aktion sei ein „Verbrechen gegen die Informationsfreiheit" gewesen, so wird im Clip ausgeführt, weshalb aus Protest nun Websites der Regierung und regierungsnaher Organisationen lahmgelegt würden. Die meisten der Betroffenen wie etwa der Geheimdienst Säpo bestätigten die Atta-

---

34 BKA, Hackaktivisten, S. 70.

35 Siehe den Bericht in http://www.stern.de/wirtschaft/unternehmen/541977.html?nv=cb.

36 Siehe die Stellungnahme des Neiman Marcus unter: http://www.neimanmarcus.com/en-ca/NM/Security-Info/cat49570732/c.cat?icid=topPromo_hmpg_ticker_SecurityInfo_0114

37 http://www.h-online.com/security/news/item/Carberp-trojan-nets-criminals-almost-Lb170-million-1839746.html.

cken als Ursache der Störungen. Die Polizei vermutet eine Protest-Aktion gegen die von der schwedischen Regierung geforderte Auslieferung des Wikileaks-Gründers Julian Assange.[38] Am 19. März 2013 wurde eine DNS-DDoS-Attacke auf die unabhängige Antispam-Organisation Spamhaus durchgeführt. Dieser Angriff, der auch Spamhaus-Partner in den Vereinigten Staaten, den Niederlanden und Großbritannien betraf, wird von Experten als die bislang heftigste Distributed-DoS-Attacke in der Geschichte des Internets angesehen. Spamhaus hatte zuvor die IP-Adressblöcke des als Spammer-freundlich bekannten niederländischen Hosters Cyberbunker auf seine Blacklist gesetzt. Weil nahezu 80 % aller Antispam-Filter diese Liste einsetzen und damit den Hoster nun blockten, konnten Kunden von Cyberbunker plötzlich kaum noch Mails versenden. Ein 35-jähriger Niederländer, der verdächtigt wird, an dem Angriff beteiligt zu sein, wurde in seinem Haus in Barcelona festgenommen. Er soll an die Niederlande ausgeliefert werden und sich dort vor Gericht verantworten.[39]

Im Jahre 2014 gab es in Deutschland über 32.000 DDoS-Angriffe in nahezu allen Branchen. Ein Viertel der betroffenen Unternehmen war über die Netzinfrastrukturen angegriffen worden.[40]

Oft wird Software manipuliert, um schnell an Geld zu gelangen. Im Rahmen eines Ermittlungsverfahrens der Abteilung für organisierte Kriminalität der Staatsanwaltschaft Essen und des Polizeipräsidiums Gelsenkirchen wurden Ende Januar 2015 in mehreren Städten Nordrhein-Westfalens und in fünf weiteren Bundesländern zeitgleich Haftbefehle und Durchsuchungsbeschlüsse vollstreckt. Hintergrund war die professionelle Manipulation der Software von Geldspielgeräten, um Einfluss auf die Gewinnausschüttung zu nehmen. Insgesamt waren 125 Objekte betroffen. Die Schadenssumme ist gleichwohl noch nicht bekannt.[41]

Sicherheitslücken werden von Betrügern benutzt, um Dialer in PCs einzuschleusen. Die Hamburger Staatsanwaltschaft hat in einem Fall festgestellt, dass mit Hilfe manipulierter Websites eine international agierende Gruppe einen Trojaner auf dem Rechner des Opfers platzierte. Dieser enthielt einen Dialer, den er im Hauptverzeichnis des Windows-PCs ablegte. Sodann aktivierte er den Dialer und sorgte für eine kurze vom Nutzer unbemerkte Einwahl bei einer Frankfurter Nummer. Anschließend erhielt das Opfer eine Rechnung, mit der es zur Zahlung von 69,95 Euro aufgefordert wurde, wegen der angeblichen Nutzung eines Monats-Abonnements für ein Online-Erotik-Angebot. Mehr als 100.000 Rechnungen sollen von einer Abrechnungsfirma für diesen "Service" versandt worden sein. Auf diese Weise erwirtschafteten die Betrüger bis Mitte 2003 mindestens 1,8 Millionen Euro Um-

38 http://heise.de/-1724615.

39 http://www.om.nl/actueel/nieuws-persberichten/@160856/nederlander/.

40 Die Lage der IT-Sicherheit in Deutschland 2014 S. 21.

41 http://www.presseportal.de/blaulicht/pm/51056/2936630#.

satz. Der geständige Geschäftsführer der Firma wurde im Juni 2005 zu einer Freiheitsstrafe von einem Jahr auf Bewährung verurteilt.[42]

Das Internet ermöglicht auch die Verbreitung von Viren. Im Mai 2004 hatte sich der Wurm "Sasser" über Schwachstellen von Betriebssystemen in Rechner eingeschleust. Dadurch schalteten sich die Computer selbstständig ab. Der Wurm verbreitete sich durch das Internet und infizierte weitere Computer. Allein bei der EU-Kommission in Brüssel waren 1.200 PCs betroffen. Das Reservierungssystem von Delta Airlines war sieben Stunden außer Betrieb, 40 Flüge mussten annulliert werden. Der Virus "Netsky" attackierte die Computer per Email und störte – unter anderem – Computeranlagen in zwei Bildungseinrichtungen und einer Medizinfirma. Die beiden Viren haben weltweit Computersysteme lahmgelegt, und ihr Programmierer, der zur Tatzeit 17 Jahre alt war, wurde im Juli 2005 vom LG Verden zu einer Jugendstrafe von einem Jahr und neun Monate verurteilt. Die Strafe wurde zur Bewährung ausgesetzt.[43]

Ende 2013 wurden gefälschte Emails an zahlreiche Internetnutzer geschickt, in denen das BKA als Absender ausgegeben wurde. Der Mail-Betreff lautete „Vorladungstermin Polizei/BKA“. „Die Mail-Adresse erweckte den Eindruck, als käme sie vom Bundeskriminalamt.“ Das war allerdings nicht der Fall. In der E-Mail ging es um einen angeblichen Warenbetrug im Internet. Der Empfänger wurde aufgefordert, einen Link anzuklicken, um einerseits mehr über Vorwürfe gegen ihn selbst zu erfahren. Andererseits sollte er herausfinden können, ob er selbst Opfer des Warenbetrugs geworden sei.

Der Link führte auf eine Webseite, die unter Umständen Schadsoftware auf dem Rechner installierte – etwa um anschließend Passwörter abzufischen oder den Rechner zu kapern. Das BKA hat den Empfänger geraten, die E-Mail sofort zu löschen.[44]

In den letzten zehn Jahren hat sich die Zahl jener vermehrt, die die Möglichkeiten des elektronischen Geschäftsverkehrs nutzen. Im Jahr 2004 haben 22,7 Millionen Bürger in Deutschland Waren online – etwa Bücher, Computerspiele, Autos oder Medikamente – gekauft. Ein großer Teil der Internetnutzer informiert sich über Reiseangebote, Telekommunikationsprodukte, Computersoftware und auch über Mode. Deutschland nimmt – nach Angaben einer Studie des „Bundesverbandes Digitale Wirtschaft“ – beim Internet-Einkauf den dritten Platz innerhalb der EU-Länder ein.[45]

Im Jahr 2014 ist der Onlinehandel um knapp 25 % auf 48,8 Milliarden Euro gewachsen. Im Jahr 2013 lag die Wachstumsrate den Zahlen des BVH zufolge bei knapp 42 %, das waren 39,1 Milliarden Euro. Darin nicht enthalten sind digitale Güter wie e-Books, Musik oder Software und Dienstleistungen wie Fahrscheine,

---

42 http://www.heise.de/newsticker/Erste-Freiheitsstrafe-wegen-Dialer-Betrugs--/meldung/60377.

43 Siehe dazu http://www.dw-world.de/dw/article/0,1564,1644265,00.html; http://www.heise.de/newsticker/Meldung/61416.

44 http://www.bsi-fuer-buerger.de/

45 BVDW, E-Commerce, 2005, S. 9.

Flugtickets, Reisen und Konzertkarten. Damit wurden noch einmal 10,6 Milliarden Euro Umsatz gemacht. Der Anteil des Versandhandels am gesamten Einzelhandel (ohne Lebensmittel, steuerbereinigt) stieg im Jahr 2013 von 9,4 % auf 11,2 %.[46]

Auch die Kriminellen versuchen, dieses Wachstum zu ihren Gunsten zu missbrauchen. Diese – in den letzten Jahren besonders hervorgetretene – Deliktsgruppe steht in Zusammenhang mit dem elektronischen Handel und stellt – nach einer Statistik des LKA Brandenburg – ein sich sowohl qualitativ als auch quantitativ stark weiterentwickelndes Kriminalitätsfeld dar. In den meisten Fällen bieten die Täter gegen Bargeld über Internetplattformen Waren an, die gar nicht in ihrem Besitz sind. In anderen Fällen versuchen die Täter Waren zu erhalten, ohne dafür den entsprechenden Preis zu bezahlen. Oft werden dabei Kontonummern aus weggeworfenen Überweisungsträgern verwendet.[47]

Eine kriminelle Bande hatte in einem Internet-Auktionshaus fremde Anbieterkonten gehackt und darin nicht existierende Waren wie Elektronikartikel, Computerzubehör, Spiele oder Markenkleidung angeboten. Weit über 1.000 Kunden fielen darauf herein. Der Schaden hierbei lag bei 100.000 Euro. Der 34-jährige Drahtzieher der Internet-Hackerbande ist vom Landgericht Bonn wegen Betrugs und Urkundenfälschung in fast 500 Fällen zu sechs Jahren Haft verurteilt worden.[48]

Ende April 2017 ist es den Staatsanwälten der Zentralstelle Cybercrime Bayern und der Kriminalpolizeiinspektion Fürstenfeldbruck in Zusammenarbeit mit Polizeikräften aus Nordrhein-Westfalen gelungen, ein Netz von Fakeshop-Betreibern zu zerschlagen. Als „Fakeshops" werden betrügerische Angebote im Internet bezeichnet, bei denen die Täter Waren gegen Vorkasse zum Kauf anbieten, in der Folge die Vorkasse der getäuschten Kunden vereinnahmen und den Versand der bestellten Waren schuldig bleiben. „Fakeshops" unterscheiden sich kaum von seriösen Verkaufsplattformen im Internet. Drei Personen wurden in Nordrhein-Westfallen festgenommen. Die Beschuldigten sind dringend verdächtig, mindestens 75 sogenannte Fakeshops im Internet eröffnet zu haben. Sie sollen auf professionell gestalteten Internetseiten überwiegend hochwertige Konsumgüter angeboten haben. Jeweils in dem Glauben an seriöse Kaufangebote bestellten die Geschädigten die angebotenen Gegenstände und überwiesen den verlangten Kaufpreis, ohne jedoch tatsächlich Waren zu erhalten. Im Rahmen der Ermittlungen wurden rund 100 falsche Personen- und Adressdaten bekannt, die von den Beschuldigten für den Betrieb der „Fakeshops" und zudem für eigene betrügerische Bestellungen im Internet verwendet worden sein sollen. Bankkonten wurden unter falschen Personalien eröffnet. Die Schadenssumme

---

46 http://www.bevh.org/presse/pressemitteilungen/details/datum/2014/februar/artikel/ergebnisse-der-bvh-b2c-studie-2013-liegen-vor-interaktiver-handel-2013-massive-umsatzsteigerungen/?cHash=9ede2a68b8eb6f23ccbe826deff4ae3c

47 Pressemitteilung des LKA Brandenburg v. 18.4.2005

48 http://www.datenschutzticker.de/index.php/2013/03/landgericht-bonn-sechs-jahre-haft-fuer-internet-hackerbanden-chef/

liegt nach derzeitigem Ermittlungsstand bei mindestens 220.000 EUR. Es konnten 500 Geschädigte im In- und Ausland ermittelt werden.[49]

Die elektronischen Plattformen dienen auch als Marktplätze, über die Produktfälschungen angeboten werden. Nach Schätzungen von Experten sind etwa 50 % der bei Internetauktionen angebotenen Artikel Fälschungen. Mitte Juni 2005 wurden 14 Wohnungen und Büros in acht deutschen Städten durchsucht. Die Ermittler konnten beweisen, dass eine Gruppe von Kriminellen Luxusartikel der Marke JOOP gefälscht und anschließend über eBay versteigert hatte. Die Einnahmen durch den Verkauf der ca. 76.000 Artikel beliefen sich auf ungefähr 2,3 Millionen Euro. 69 Personen in 27 deutschen Städten sollen beteiligt gewesen sein. Der Kopf der Bande wurde in Istanbul vermutet, von wo aus die Fälschungen nach Deutschland versandt wurden.[50] Anfang Dezember 2014 wurden von EUROPOL 292 Internet Domains beschlagnahmt, die gefälschte Luxusartikel, Sportbekleidung, Elektronikgeräte, Arzneimittel, raubkopierte Filme und Musik verkauften. Obwohl niemand festgenommen wurde, versuchen die Strafverfolger die Geldflüsse nachzuverfolgen.[51]

Oft wird auch Diebesgut über Online-Marktplätze veräußert, die nach BGH die Straftatbestände der gewerbsmäßigen Hehlerei und des versuchten Betruges erfüllen.[52] Außerdem sind Fälle bekannt, in denen ein eBay-Mitglied sein Konto zur Verfügung gestellt hat, damit darüber Diebesgut angeboten werden kann. Auch in solchen Fällen hat der BGH Begünstigung gemäß § 257 Abs. 1 StGB festgestellt.[53]

Nach Angaben der WHO sind 6 % der Arzneimittel, die weltweit verkauft werden, Fälschungen.[54] Nach einer Studie des Europarates steigt die Vermarktung von gefälschten Medikamenten in Deutschland jährlich um 5 %.[55] Dass der Online-Versand hier eine wichtige Rolle spielt, liegt auf der Hand. Ende Juli 2005 hat sich im Zuge eines staatsanwaltlichen Ermittlungsverfahrens in Saarbrücken herausgestellt, dass auf Internetbestellung teure gefälschte Medikamente versandt wurden, die entweder völlig wirkungslos oder gesundheitsgefährdend waren.[56]

Die Nutzung des Internets für "day-to-day-business" hat in den letzten sieben Jahren einen neuen Tätigkeitsbereich für Kriminelle eröffnet. Die "Cyber-Umgebung" selbst ist in solchen Fällen nicht das Ziel von Angriffen. Die Kriminellen missbrauchen sie nur, um Straftaten vorzubereiten oder diese in ein Versuchsstadium zu bringen. Es

---

[49] S. Pressemitteilung 5/17, von der StA Bamberg.

[50] Dazu http://www.onlinemarktplatz.de/modules.php?name=News&file=article&sid=1314.

[51] https://www.europol.europa.eu/content/292-internet-domain-names-seized-selling-counterfeit-products

[52] S. BGH, 27.8.2008 – 2 StR 329-08, MMR 208, 728 f.

[53] BGH, 29.4.2008 – 4 StR 148/08, K§R 208, 533, s. dazu auch *Schlömer*/*Dittrich,* K§R 2009, S. 147.

[54] http://www.who.int/medicines/organization/qsm/activities/qualityassurance/cft/CounterfeitOverview.htm

[55] Council of Europe, Counterfeit Medicines, Survey Report, S. 27.

[56] Dazu http://www.justiz-spzoales.saarland.de/detail.htm?mid=7884.

handelt sich dabei um die Konstellation, in der das Internet als „Tatmittel“ benutzt wird.

Ein Beispiel für den Missbrauch der "Cyber-Umgebung" ist die Zusendung von „Spam“. Nach Angaben der OECD handelt es sich bei der Hälfte allen E-Mail-Verkehrs um Spam.[57] Es wird geschätzt, dass im Jahre 2003 4,9 Trilliarden Spammails gesendet wurden;[58] allein AOL gibt an, dass im April 2003 2,37 Billionen Spammails pro Tag abgeblockt wurden.[59] Die Firma Brightmail, ein Entwickler von Softwarefiltern, prüfte im Jahr 2004 über 106 Milliarden Spammails aus der Internetkommunikation und stellte fest, dass die meisten Spammails Produkte oder Dienstleistungen anbieten.[60] Es folgen Dienstleistungen für Erwachsene und die sog. Nigeria-E-Mails.[61] Im Juli 2009 wurde 89 % aller E-Mails als Spam registriert.[62]

Die Spam-Flut hat Firmen in Europa im Jahr 2002 $ 2,5 Milliarden und in den USA im Jahr 2003 $ 10 Milliarden gekostet. Faktoren, die hier berechnet wurden, waren:

- die Zeit, die von den Arbeitnehmern verwendet wird, um die Werbe-E-Mails zu checken und auszusortieren,
- die Kosten, die durch die zusätzlichen Computer- und Netzwerkressourcen entstehen, die für die Bewerkstelligung von Werbe-E-Mails erforderlich sind, und
- die finanziellen Investitionen in technische Maßnahmen wie Filter und in Arbeitsleistungen, die sich mit der Abwehr von Angriffen durch Werbe-E-Mails beschäftigen.[63]

In seinem Spam-Bericht für September stellte Kaspersky fest, dass deutsche Internet-Nutzer weltweit die meisten schädlichen Anhänge und Links in ihren Postfächern vorfanden und lösten damit die USA an der Spitze ab. Neben dem höheren Aufkommen an gefährlichem Spam haben sich die Methoden verändert: Die Absender geben sich politischer.[64]

---

57 Siehe dazu OECD, Background Paper for the OECD Workshop on Spam, S. 4.

58 *Gauthroner*/*Drouard*, Unsolicited Commercial Communiacations and Data Protection S. 67.

59 *Krim,* Spam Cost to Business Escalates, Washington Post v. 13.3.2003.

60 Siehe die detaillierte Darstellung in: Brightmail's Prove Network, The State of Spam – Impact and Solutions.

61 Nigeria-E-Mails sind E-Mails, die dem Empfänger eine große Geldsumme versprechen, wenn er z. B. afrikanischen Geschäftsleuten, einer Diktatorenwitwe oder einem verschollenen Prinzen helfen würde, riesige Beträge – regelmäßig Millionen Dollar – außer Landes zu schaffen. Der E-Mail-Empfänger soll - nach dem Inhalt der E-Mail – sein Konto kurzfristig zur Verfügung stellen, um die Millionen für kurze Zeit "zu parken". Geht der Internetnutzer auf diese E-Mail ein, dann wird eine "geringe Gebühr" für das gewinnbringende Geschäft verlangt, z. B. für Überweisungen, Anwaltskosten oder Steuern, die oft einige tausend Dollar hoch sein können. Dass die versprochenen Millionen nie ausgezahlt werden, versteht sich von selbst.

62 S. Symantec, Spam Report, August 2009, S. 4.

63 Siehe dazu *Krim*, Spam Cost to Business Escalates, Washington Post, 13.3.2003.

64 Kaspersky lab, Spam im September 2012

Auch die Android-Betriebssysteme sind vom Spam betroffen. In den USA breitet sich ein neues Botnetz für solche Systeme namens Spamsoldier aus. Das Botnetz verbreitet sich durch SMS, die Gratisversionen von Spielen wie Need for Speed oder Angry Birds Space versprechen. In der SMS werden die Spiele über Links zum Download angeboten. Sobald ein Nutzer dem Link folgt, installiert sich der als App getarnte Trojaner – teilweise werden auch wirklich Gratisspiele zur Ablenkung des Nutzers mitgeliefert. Der Trojaner nimmt dann Kontakt mit einem Command-and-Control-Server auf. Dieser schickt Spamsoldier eine Liste von 100 Mobilfunk-Rufnummern in den USA und eine passende Spam-SMS, die der Bot nun – so schnell es das Mobiltelefon erlaubt – an die Liste schickt. Sind die 100 Nummern abgearbeitet, lässt sich die Schadsoftware neue Listen vom C&C-Server schicken, bis dieser nicht mehr antwortet oder neue Befehle gibt. Seine Aktivität versucht der Trojaner kontinuierlich zu verschleiern. Alle ausgehenden Spam-SMS werden gelöscht. Antwortende SMS auf den Spam versucht das Programm ebenfalls zu entfernen.[65]

Das Bundesamt für Sicherheit in der Informationstechnik hat in seiner Zusammenfassung der IT-Sicherheitslage in Deutschland festgestellt, dass sich im Jahr 2014 bezüglich der Spam-Zahl mit einem deutlichen Zuwachs von ca. 80 % im Vergleich zum Vorjahr eine Trendwende bei den seit Jahren stagnierenden Zahlen abzeichnet.[66]

Eine andere Missbrauchsform der Cyber-Umgebung ist die Zusendung von „Phishing-Mails", nämlich der Versuch der Entwendung vertraulicher Daten von Internet-Nutzern – z. B. Kreditkartennummern, Bankverbindungen, TAN oder PIN. Nach Angaben der „Anti-Phishing-Working-Group" ist ein Zuwachs an Vorfällen bis zu monatlich 24 % festzustellen.[67] Nach dem Phishing Activity Report, von Juli 2005 haben 85,9 % der „Phishing-Mails" als Ziel die Erlangung von Online-Banking-Zugangsdaten.[68] Man hat errechnet, dass im Jahr 2003 den Finanzdienstleistern und Kreditkarteninhabern durch Phishing Schäden in Höhe von $ 1,2 Milliarden entstanden sind.[69] Im Jahr 2007 ist die Zahl der Phising-Fälle bei Onlinebanking gestiegen. Bundesweit hoben Kriminelle in mehr als 4.100 Fällen rd. € 10 Mio. von Konten der Geschädigten ab. Die Schadenssumme liegt um ein Viertel höher als 2006. Auch international haben die Phising-Betrugsversuche zugenommen. Die APWG registrierte in ihrer Statistik vom Dezember 2007 weltweit über 25.000 Attacken pro Monat.[70]

Wie der Präsident des Bundeskriminalamtes (BKA), Jörg Ziercke mitteilte, lag 2006 die Schadenshöhe aus den Phising-Fällen im Durchschnitt noch bei 2.500

---

65 https://blog.lookout.com/blog/2012/12/17/security-alert-spamsoldier/

66 Die Lage der IT-Sicherheit im Deutschland 2014, S. 15:

67 S. www.antiphishing.org.

68 Phishing Activity Report, July 2005, S. 2.

69 *Gartner*, Phishing Victims Likely Will Suffer Identity Theft Fraud, S. 5.

70 S. MMR Aktuell, XVI MMR 10/2008.

Euro, während im Jahr 2008 es schon 4.000 bis 4.500 Euro pro Fall waren. „Nach Schätzungen waren im Jahr 2008 mehr als 750.000 Computer in Deutschland mit Schadprogrammen infiziert, etwa 150.000 Rechner werden von Kriminellen unbemerkt ferngesteuert."[71]

Auch Microsoft wurde Opfer von Phishing-Attacken. Im Rahmen von Phishing-Attacken auf E-Mail- und Social-Media-Konten von Mitarbeitern des Konzerns Anfang des Jahres sind auch sensible Daten zu Anfragen von Polizeibehörden abhandengekommen. Nach Angaben des Konzerns seien die Vorgänge dem derzeitigen Informationsstand nach Teil der Angriffe der Syrian Electronic Army gewesen. Die Aktivistengruppe, die dem Assad-Regime nahestehen soll, hatte Anfang des Jahres mehrfach Blogs von Microsoft verändert und angekündigt Internet-Konten von Microsoft-Angestellten gehackt.[72]

Über Phishing-Attacken haben Cyberkriminelle sich Zugriff auf Computer von Angestellten einer ukrainischen Bank verschafft und diese mit einem Schadprogramm infiziert. Dadurch kontrollierten sie Überwachungskameras und Geldtransfersysteme. Auf diese Weise manipulierten sie die Buchhaltungssysteme vieler Banken, erhöhten die Kontosaldi und überwiesen anschließend die Differenzbeträge auf Konten in China oder in die USA. Von dort wurde das Geld dann durch kontrollierte Geldautomaten an die Täter ausgezahlt. Der Schaden wurde auf $ 1 Milliarde geschätzt. Laut Europol und Interpol ist dieser Fall der größte bekanntgewordene Cyber-Bankraubüberfall, in dem bis zu 100 Geldinstitute in über 20 Ländern angegriffen wurden. Die Täter begannen mit ihren Vorbereitungen Ende 2013, bis sie Anfang 2015 aufgedeckt wurden.[73]

Anfang Dezember 2016 hat ein international besetztes Ermittler-Team mehrere Betreiber der Botnet-Gang Avalanche, die eine der größten Botnet-Infrastrukturen weltweit betreibt, verhaftet. Die Ermittler haben hunderttausende Domains und 39 Server beschlagnahmt, die im Zusammenhang mit dem Botnet zum Einsatz kamen. Nach Angaben der StA Verden, die an die Ermittlungen teilnahm, war der Erfolg das Resultat aus einer mehr als vier Jahre andauernden, grenzübergreifenden Ermittlungsarbeit, an der auch die Zentralinspektion Lüneburg, das FBI und weitere US-Behörden sowie Sicherheitsbehörden von 39 Staaten beteiligt waren. Die Ermittler konnten 16 Mitglieder der Avalanche-Führungsebene aus zehn Ländern identifizieren. Zum Zeitpunkt des Zugriffs sollen allein in Deutschland über 50.000 Rechner unter der Kontrolle des Botnetzes gestanden haben. Die Täter waren mindestens seit 2009 aktiv und nutzten ihre Botnet-Infrastruktur zum Versand von Phishing- und Virenmails. Pro Woche sollen sie über eine Million Mails verschickt haben. Im Jahr 2010 war Avalanche für zwei Drittel aller Phishing-Angriffe verantwortlich. Laut StA sollen sie von Online-

71 Neue Osnabrücker Zeitung v.15.3.2008.

72 http://www.securityweek.com/hackers-steal-law-enforcement-inquiry-documents-microsoft

73 http://newsroom.kaspersky.eu/de/texte/detail/article/der-grosse-bankraub-cybergang-carbanak-stiehlt-eine-milliarde-us-dollar-von-100-finanzinstitut.

Banking-Nutzern durchschnittlich um mehr als 5000 Euro entwendet haben. Der Staatsanwaltschaft liegen Anzeigen über 1336 Taten vor mit einer Schadenssumme von insgesamt etwa sechs Millionen Euro.[74]

Oft wird Erpressungs-Malware automatisch eingesetzt. Die Antivirenexperten von Trend Micro haben einen Lösegeld-Trojaner entdeckt, der den Boot-Vorgang blockiert. Der Schädling führt einen Neustart durch und fordert den Nutzer auf, ein Lösegeld in Höhe von 920 Hrywnja (ukrainische Währung, umgerechnet rund 90 Euro) über den Zahlungsdienstleister QIWI an die Erpresser zu zahlen.[75]

Das Landgericht Gießen hat Ende Juni 2014 fünf junge Männer aus Mecklenburg-Vorpommern und drei weiteren Bundesländern schuldig gesprochen, bundesweit mehr als 40 Online-Shops lahmgelegt und deren Betreiber erpresst zu haben. Die Richter erkannten unter anderem auf Computersabotage und Erpressung. Einer der Angeklagten erhielt ein Jahr und zehn Monate Haft auf Bewährung, die übrigen wurden nach Jugendstrafrecht verurteilt und erhielten bis zu eineinhalb Jahre auf Bewährung. Die Täter hatten die Shops zwischen 2010 und 2011 attackiert und mit unzähligen Anfragen die Server der Firmen lahmgelegt. Danach forderten sie von den Betreibern 100 bis 350 Euro, damit sie die Angriffe beenden. Allerdings ging nur ein kleiner Teil darauf ein. Die Umsatzeinbußen der Shop-Betreiber sollen im sechsstelligen Bereich liegen.[76]

US-Hacker behaupteten, sich über die Server der Finanzprüfer PriceWaterhouse-Coopers Zugriff auf die Steuerunterlagen von Mitt Romney verschafft zu haben, dem Präsidentschaftskandidaten der Republikaner 2012. Die Hacker wollten verschlüsselte Kopien der Unterlagen an zahlreiche US-Medien verschickt haben und drohten mit der Freigabe der Schlüssel. Der wegen seines Steuersatzes von 13 % oftmals kritisierte Romney könne die Veröffentlichung aber mit einem Schweigegeld verhindern – in Höhe von einer Million Dollar. Ob die Hacker tatsächlich brisantes Material in Händen gehalten haben, ist noch unklar. Der Secret Service soll Ermittlungen in der Sache angestellt haben. PriceWaterhouseCoopers teilte mit, keinen Hinweis auf einen Einbruch in das eigene Computersystem gefunden zu haben.[77] Im März 2013 warnte der BKA vor einer neuen Variante des BKA-Trojaners, die den Rechner von betroffenen Computeranwendern sperrt und eine Art Lösegeld einfordert. Ähnlich wie bei einer früheren Variante, erscheint, wenn der Rechner infiziert ist, auf dem Bildschirm ein nicht wegzuklickendes Fenster. Diesem wird durch Anzeige des Logos der BKA-Pressestelle ein vermeintlich offizieller Anstrich gegeben, erklärte das Bundeskriminalamt. Dabei werde behauptet, dass die Funktion des Computers "aus Gründen unbefugter Netzaktivitäten ausgesetzt" sei. Außerdem werden Rechtsver-

---

74 https://www.europol.europa.eu/newsroom/news/%E2%80%98avalanche%E2%80%99-network-dismantled-in-international-cyber-operation

75 Siehe Malware blockiert Bootvorgang, Heise 13.4.2012.

76 Dazu siehe: http://www.hr-online.de/website/rubriken/nachrichten/indexhessen34938.jsp?rubrik=36090&key=standard_document_52202697&tl=rs

77 http://h-online.com/-1702616

letzungen angeführt, die die vermeintliche Ursache für die Sperrung sein sollen. Bei der aktuellen Variante der Schadsoftware werden vier Fotos eingeblendet. Dabei handelt es sich um eine strafbewehrte jugendpornografische Darstellung. Im weiteren Text wird behauptet, dass „die Wiedergabe von pornografischen Inhalten mit Minderjährigen festgestellt" worden sei. Der Nutzer werde aufgefordert, 100 Euro über die Zahlungsdienstleister uKash oder Paysafecard zu zahlen, um einen Freigabecode zur angeblichen Entsperrung des Rechners zu erhalten. Gleichwohl ist der Rechner in diesem Fall schon infiziert und wird auch durch eine Zahlung des Lösegelds nicht wieder sauber.[78]

Der Erpressungs-Trojaner Bitcrypt verschlüsselte Dateien des Anwenders und gab sie nur gegen Zahlung von 260 Euro Lösegeld frei. Nach der Überweisung haben die Erpresser dem Anwender das zugehörige Entschlüsselungsprogramm gesendet, das die Daten wieder dechiffrieren ließ. Sicherheitsexperten haben jedoch das Programm geknackt und das profitable Geschäft gestoppt.[79]

Im Dezember 2014 hatten Online-Erpresser Kryptofunktionen in eine Web-Anwendung eines europäischen Finanzdienstleisters gebaut und verschlüsselten alle Daten, die in der Datenbank gespeichert waren. Anschließend forderten die Täter Lösegeld in Höhe von 50.000 $.[80]

Insgesamt haben Cyberkriminelle durch Erpessungs-Software von April 2014 bis Juni 2015 – laut Angaben des FBI – $ 18 Millionen erpresst. Die Lösegeld-Transfers erfolgten meist über Bitcoin, die Mittelsmänner entgegennahmen und dann über ihre Bankkonten oder Transferdienste wie Western Union überwiesen.[81]

In ihrer Studie „Bedrohungen 2012" hat die Sicherheitsfirma McAfee betont, dass die Angriffe gegen industrielle Steuerungssysteme zunehmen werden. Die Studie berichtet vor allem über das Problem der "eingebetteten Hardware", nämlich über die produktiven Komponenten, die mit üblichen informationsverarbeitenden Komponenten vernetzt sind. Diese Malware ist in der Lage, die Steuerungen für industrielle Fertigungsanlagen anzugreifen.[82]

Im Oktober 2012 ist die US-amerikanische Federal Trade Commission (FTC) zusammen mit Kollegen aus fünf Ländern (Kanada, Australien, Irland, Neuseeland und Großbritannien) gemeinsam gegen eine Reihe von Telefon-Scammern vorgegangen. Den Beschuldigten wird vorgeworfen, zehntausenden Computernutzern vorgetäuscht zu haben, dass ihr Rechner von Malware befallen sei. Die Beschuldigten sollen ihre Herkunft verschleiert haben, indem sie Briefkastenfirmen unterhielten, 80 verschiedene Domains und 130 Rufnummern nutzten. Sie sollen sich be-

---

78 http://www.bka.de/nn_233148/DE/Presse/Pressemitteilungen/Presse2013/130322__Warnmeldung__Ransomware.html

79 http://blog.cassidiancybersecurity.com/post/2014/02/Bitcrypt-broken

80 https://www.htbridge.com/blog/ransomweb_emerging_website_threat.html.

81 http://www.ic3.gov/media/2015/150623.aspx.

82 McAffe, Bedrohungen 2012, 2012.

trügerisch als Anrufer im Auftrag eines renommierten Unternehmens wie Microsoft, Dell oder McAfee ausgegeben und bereitwillige Windows-Nutzer am Telefon zum Ereignisprotokoll ihres Betriebssystems gelotst haben. Anhand der dort aufgeführten möglichen gewöhnlichen Fehler- und Warnhinweise wurde den Nutzern suggeriert, dass ihr Computer mit Malware infiziert sei. Die Betrüger hätten gegen einen Betrag von 50 bis zu 450 US-Dollar angeboten, die vermeintliche Infektion zu beseitigen. Dafür sollten die Nutzer eine Software herunterladen, die angeblich die Malware beseitigt. Über diese Software hatten die Betrüger dann stattdessen Fernzugriff auf die Rechner der Betrogenen gewonnen und konnten so Software auf die betroffenen Rechner laden. In anderen Fällen hat eine betrügerische Firma auf Google Anzeigen geschaltet, die die vermeintliche Rufnummer des Supports eines IT-Unternehmens anzeigte. Verdächtigte Unternehmen in Indien seien direkt nicht anzugehen gewesen; wenn diese aber US-Telefonunternehmen für ihre Machenschaften genutzt hätten, seien die Rufnummern von den Unternehmen blockiert worden. Die australische Behörde Australia Communication and Media Authority (ACMA) schildert, tausende Telefonkunden, die sich in das Register "Do not call" eingetragen hatten, hätten sich seit 2009 vermehrt über Anrufe beschwert. Diesen Fällen sei die ACMA nachgegangen und habe diese an die FTC weitergeleitet. Australien gehörte demnach zu den ersten Zielen der Telefon-Scammer.[83]

Die Malware wird auch für Zwecke der Industriespionage eingesetzt. Das Ziel ist Know-how des Konkurrenten anzuzapfen, um so Entwicklungskosten zu sparen und ähnliche Produkte schnell und günstig auf den Markt zu bringen. Nach der neuen Studie von Corporate Trust „Industriespionage 2012“ entsteht der deutschen Wirtschaft durch Industriespionage jährlich ein Gesamtschaden von ca. 4,2 Milliarden Euro. Es wurden Daten von circa 600 vorwiegend mittelständischen Unternehmen erhoben, die belegen, dass das Bedrohungspotential durch kriminelle Handlungen im Internet in den vergangenen Jahren um 50 % gestiegen ist.[84]
Die sog. Cyberspionage-Kampagne horcht seit 2004 systematisch bis zu 1.000 Personen aus mindestens 40 Ländern aus. 350 der ausspionierten Personen, die identifiziert werden könnten, bekleiden wichtige Positionen in privaten und öffentlichen Einrichtungen, Regierungsinstitutionen, Forschungseinrichtungen oder der Rüstungsindustrie. Außerdem wurden auch Tibet-Aktivisten angegriffen. Die als NetTraveler benannte Kampagne beschaffte sich so vor allem Informationen aus den Bereichen der Weltraumforschung, Nanotechnologie, Energieproduktion, Nuklearenergie, Lasertechnologie, Medizin und Kommunikation. Die Opfer infizierten sich mit der Spionagesoftware über gezieltes Phishing (Spear Phishing). Von den 350 identifizierten Opfern in 40 Ländern kommen die meisten – der Anzahl nach geordnet – aus der Mongolei, Russland, Indien, Kasachstan, Kirgisistan, China, Tadschikistan, Südkorea, Spanien und Deutschland. Deutschland hat es so in die Top 10 der am meisten betroffenen Nationen geschafft.[85]

---

83 http://ftc.gov/opa/2012/10/pecon.shtm, FTC Halts Massive Tech Support Scams

84 Siehe Corporate Trust, Studie Industriespionage 2012.

85 The Nettraveler, Kaspersky Lab.