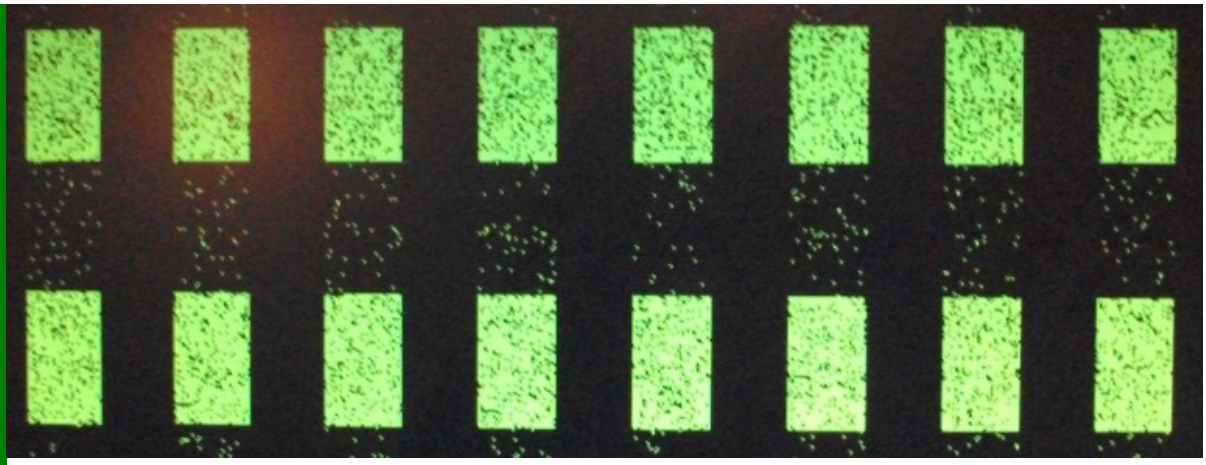


IuK-Strafrecht
System, Begriffe und Fallbeispiele

Dieter Kochheim

Cybercrime und materielles Strafrecht

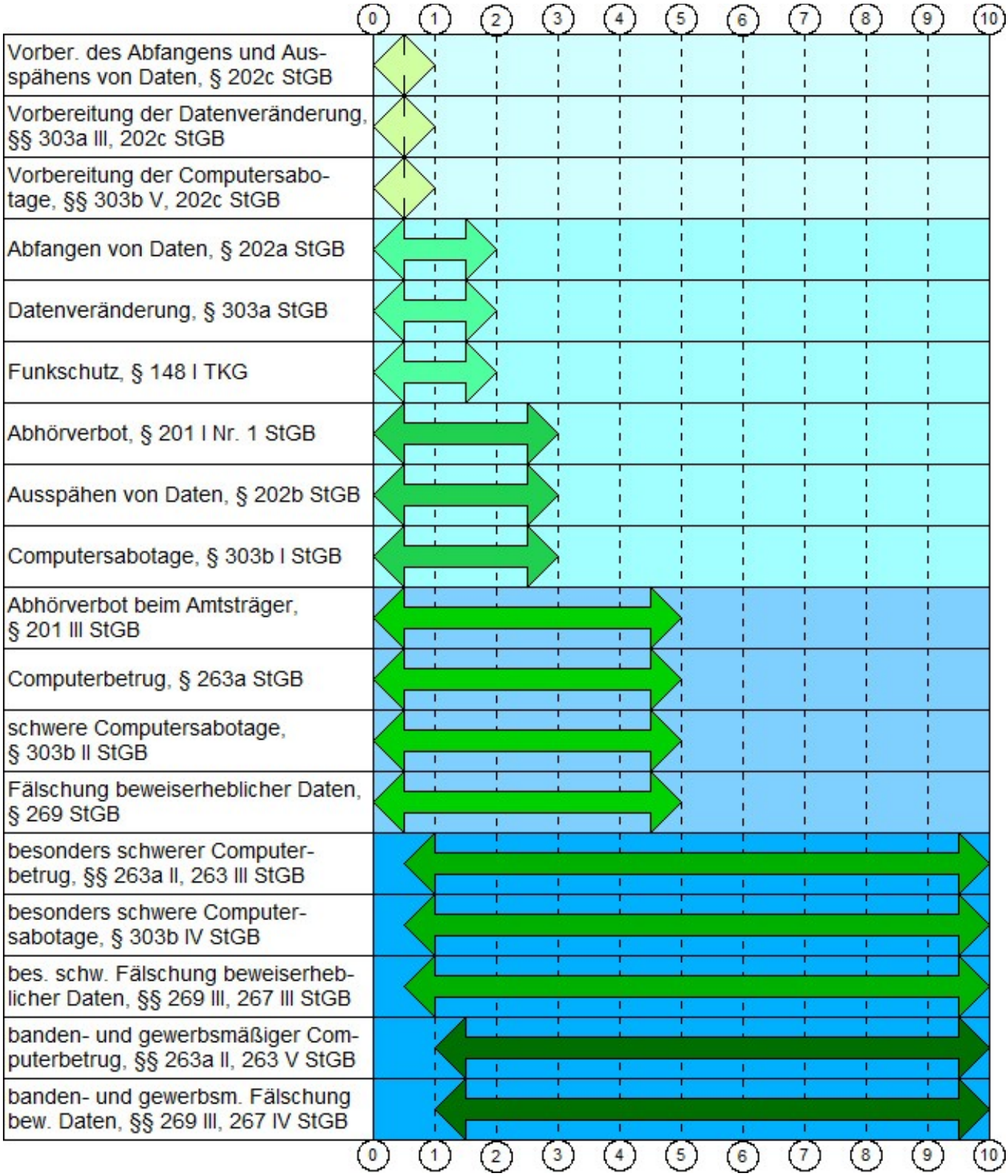
Für Marco Thelen, Bonn.

Vorreiter bei der Bekämpfung der Cybercrime.

Verstorben im September 2011 im Alter von 35 Jahren.

14.04.2012	1.05	Neues Kapitel 2.6.1.8
31.03.2012	1.04	Neue Kapitel 2.6.1, 2.7.3 und diverse Aktualisierungen
06.01.2012	1.03	Ergänzungen
29.10.2011	1.02	Neu: 2.10 (Struktur der Cybercrime); redaktionelle Korrekturen.
08.10.2011	1.01	Erweiterung von 2.4.5 (Onlinebanking); redaktionelle Korrekturen
03.10.2011	1.00	Erstveröffentlichung

Thema:	**IuK-Strafrecht**
Autor:	Dieter Kochheim
Version:	1.05
Stand:	14.04.2012
Cover:	„Breakdown“, D. Kochheim Bildschirm nach Defekt der Grafikkarte
Impressum:	**CF**, cyberfahnder.de


0
1
2
3
4
5
6
7
8
9
10
Vorber. des Abfangens und Ausspähens von Daten, § 202c StGB
Vorbereitung der Datenveränderung, §§ 303a III, 202c StGB
Vorbereitung der Computersabotage, §§ 303b V, 202c StGB
Abfangen von Daten, § 202a StGB
Datenveränderung, § 303a StGB
Funkschutz, § 148 I TKG
Abhörverbot, § 201 I Nr. 1 StGB
Ausspähen von Daten, § 202b StGB
Computersabotage, § 303b I StGB
Abhörverbot beim Amtsträger, § 201 III StGB
Computerbetrug, § 263a StGB
schwere Computersabotage, § 303b II StGB
Fälschung beweiserheblicher Daten, § 269 StGB
besonders schwerer Computerbetrug, §§ 263a II, 263 III StGB
besonders schwere Computersabotage, § 303b IV StGB
bes. schw. Fälschung beweiserheblicher Daten, §§ 269 III, 267 III StGB
banden- und gewerbsmäßiger Computerbetrug, §§ 263a II, 263 V StGB
banden- und gewerbsm. Fälschung bew. Daten, §§ 269 III, 267 IV StGB

Einleitung

Seit 2007 beschäftigt sich die Webseite cyberfahnder.de einerseits mit den technischen Fragen im Zusammenhang mit der IuK-Technik und des Internets und andererseits mit den Erscheinungsformen der Cybercrime sowie den formellen und materiellen Rechtsfragen, die mit ihr in Verbindung stehen.

Dabei ging es zunächst darum, die Grundlagen zu erarbeiten. Mit den technischen Fragen befassen sich vor allem sieben Aufsätze [1]:

- Angriffspunkte und -methoden
- Kabel und Netze
- autonome Systeme und Tiers
- Mobilfunk
- eurasische Verbindungen
- Overlay-Netze der öffentlichen Verwaltung
- Netzkommunikation

Den zweiten Schwerpunkt bilden die Erscheinungsformen der Cybercrime und ihre Strukturen:

- IT-Straftaten
- IT-Strafrecht
- Nummerntricks
- Phishing
- Skimming
- Malware
- Botnetze
- Social Engineering
- Basar für tatgeneigte Täter
- neue Hacker-Boards schirmen sich ab

Daraus entstanden die analytischen Aufsätze:

- arbeitsteiliges Skimming
- Schurkenprovider und organisierte Cybercrime
- modulare Kriminalität
- Kriminalität aus dem Baukasten

Aufbauend auf diesen Vorarbeiten ist es mir 2010 bei dem Arbeitspapier Cybercrime [2] darum gegangen, die Erscheinungsformen, Besonderheiten und Strukturen der Cybercrime zu beschreiben und für die weiteren Auseinandersetzungen zugänglich zu machen. Es ist eine notwendige Zwischenbilanz nach gut drei Jahren Cyberfahnder, die auch der Bereinigung dient. So war 2010 zum Beispiel die Urform des Phishings auf der Grundlage von E-Mails mit Formularfeldern lange überholt und an ihre Stelle waren äußerst verfeinerte Formen des Identitätsdiebstahls getreten.

Auf das Arbeitspapier Cybercrime bauen mehrere Aufsätze auf, die zunächst verschiedenen Fragen galten.

Paget von McAfee hat 2010 nicht nur die Bedeutung des Hacktivismus hervorgehoben, sondern besonders auch die mafiösen Strukturen der Cybercrime betrachtet [3]. Dieser (fast nur) in englischer Sprache verfügbare Aufsatz musste dem deutschsprachigen Publikum zugänglich gemacht werden. Ich habe ihn wertend und kommentierend nacherzählt [4] und seine wesentlichen Informationen dazu genutzt, um eine Zeitgeschichte der Cybercrime vorzustellen [5]. Diese historische Dimension hat Paget vernachlässigt und sie zeigt, dass die Cybercrime alle Entwicklungen in der IuK-Technik zeitnah begleitet und für sich nutzbar gemacht hat. Die grundlegenden Fakten und Erkenntnisse daraus sind in die Präsentation „Cybercrime und Cyberwar“ vom November 2010 eingeflossen [6], die ich im Mai 2011 aktualisiert habe [7].

Diese Präsentationen stellen die Verbindung zu einem zweiten Schwerpunkt meiner Forschungen her, die sich den Entwicklungsperspektiven im Zusammenhang mit der Cybercrime widmen. Noch ganz harmlos erscheint der Aufsatz über die Netz-

---

1 Im Original, also in diesem Werk als PDF-Dokument, sind alle Verweise mit Hyperlinks versehen, so dass sie per Klick erreichbar sind. In ausgedruckter Form ist dieser Dienst nicht verfügbar.

2 Dieter **Kochheim**, Cybercrime, 24.05.2010

3 François **Paget**, Cybercrime and Hacktivism, McAfee 15.03.2010

4 Dieter **Kochheim**, Cybercrime und politisch motiviertes Hacking. Über ein Whitepaper von François Paget von den McAfee Labs, 20.10.2010

5 Dieter **Kochheim**, Eine kurze Geschichte der Cybercrime, 23.01.2011

6 Dieter **Kochheim**, Cybercrime und Cyberwar, 17.11.2010

7 Dieter **Kochheim**, Cybercrime – Cyberwar, 02.07.2011

kommunikation [8]. Er nimmt die technischen Fragen nach der Adressierung, den Protokollen und den Funktionsweisen der Kommunikationstechnik auf, geht dann aber über die Manipulationsmöglichkeiten dazu über, zwischen kaltem und heißem Cyberwar zu unterscheiden. Ich habe schon damals den Eindruck gehabt, dass wir uns in einer Übergangsphase befinden, in der verschiedene Machtgruppen ihre Potenziale und die Anfälligkeit von Gegnern testen, um ihre künftigen Optionen zu bewerten und zu optimieren. In den Monaten um den Jahreswechsel 2010/2011 gewannen neue Interessengruppen an Bedeutung (Hacktivismus, Söldner, Wikileaks). Sie gaben den Blick frei auf Eskalationen [9], die erst nur im Kleinen wirken. Diese Aktivitäten haben seit einigen Monaten nachgelassen, aber das ist nur die sprichwörtliche Ruhe vor dem Sturm.

Die rechtliche Auseinandersetzung mit der Cybercrime habe ich lange zurückgestellt, weil sie Stückwerk gewesen wäre und ich mich nicht in der Lage sah, sie mit ihren Wechselwirkungen und mit genügend Abstand betrachten könnte.

Mit dem Arbeitspapier Skimming [10] habe ich vor zwei Jahren damit begonnen, diese besondere Erscheinungsform in ihrer rechtlichen Tiefe zu durchdringen und das auch aus beruflichem Interesse. Der Beruf mit seinen kleingliedrigen Anforderungen und das Hobby mit der Möglichkeit, großräumig die Probleme anzugehen und zu lösen, haben dabei eine fruchtbare Symbiose gebildet. Gewonnen hat dadurch besonders die berufliche Praxis: Wenn die Probleme im Großen gelöst sind, dann lösen sich die Probleme im Einzelfall schnell oder werden gar nicht erst zum Problem.

Im Zusammenhang mit der Arbeit am Cyberfahnder haben sich interessante rechtliche Probleme und Lösungen gezeigt. Nicht zuletzt deshalb erschien Ende Juli 2011 das ▸ Arbeitpapier über die verdeckten Ermittlungen im Internet. Es gibt einen Überblick über die verfahrensrechtlichen Voraussetzungen und Grenzen der technischen und personalen Ermittlungen im Internet und setzt sich dazu ausführlich mit der Rechtsprechung des BVerfG und des BGH auseinander. Besonders wichtig sind die Aufstellung über alle angesprochenen Ermittlungsmaßnahmen, die nach dem Gewicht ihrer Eingriffstiefe aufgelistet sind <S. 24>, und die systematische Auseinandersetzung mit den personalen Ermittlungen in sozialen Netzwerken und geschlossenen Benutzerkreisen.

Nach dem ▸ Arbeitspapier Skimming schließt dieses Arbeitspapier über das ▸ IuK-Strafrecht die Lücke bei der Auseinandersetzung mit dem materiellen Strafrecht. Es befasst sich zunächst mit den weit verstreuten Tatbeständen des IuK-Strafrechts im engeren Sinne, das den strafbaren Missbrauch der IuK-Technik als solches zum Gegenstand hat und vor allem auf das Eindringen und Sabotieren in Bezug auf fremde Datenverarbeitungssysteme reagiert.

Die modernen Erscheinungsformen der Cybercrime lassen sich mit den Instrumenten des IuK-Strafrechts im engeren Sinne nur unvollständig erfassen. Das liegt nicht zuletzt daran, dass dem Gesetzgeber „autonome Malware“, die selbständig Sicherheitslücken unterläuft, sich einnistet und ihre schädlichen Wirkungen fast ohne Zutun der Täter ausführt, Botnetze, Carding-Boards und Schurkenprovider unbekannt waren, als er zuletzt 2007 wesentliche Änderungen im IuK-Strafrecht einführte.

Das führt zu Lücken im strafrechtlichen System, die jedoch weitgehend von Strafvorschriften ausgefüllt werden, die nicht speziell auf die IuK-Kriminalität ausgerichtet sind. Das gilt besonders für das Fälschen von Zahlungskarten mit Garantiefunktion (§ 152b StGB), das das Skimming-Strafrecht prägt, für die Verabredung zu einem Verbrechen (§ 30 StGB), die bereits bei der Verbreitung von Malware und anderen Vorbereitungshandlungen eine strafbare Beteiligungsform schafft, und die Mitgliedschaft in einer kriminellen Vereinigung (§ 129 StGB), die besonders die Betreiber von Botnetzen und Boards treffen wird, nachdem der

---

8 Dieter **Kochheim**, Netzkommunikation, 10.07.2010

9 Dieter **Kochheim**, Eskalationen, 20.02.2011

10 Dieter **Kochheim**, Skimming, 22.04.2011

BGH die ersten Vorstöße in diese Richtung wohlwollend begleitet hat (▸ Nazipropaganda im Internetradio).

Die Beispiele, die erörtert werden, können nicht alle Varianten und Entwicklungen erfassen, in denen sich die Cybercrime äußert. Sie lassen jedoch einen Rahmen mit Ergebnissen entstehen, die am Einzelfall geprüft und präzisiert werden müssen. Am Schluss gehe ich auf die Fragen nach der (Un-) Vollständigkeit des IuK-Strafrechts, seiner Lücken und den sinnvollen Erweiterungen ein (▸ Stand und Zustand des IuK-Strafrechts).

Am Anfang dieses Arbeitspapiers stand die Überlegung, die paar Anwendungsfälle, die mir aufgefallen waren, müssten nur einmal formuliert werden und das würden höchstens 35 Seiten werden, dachte ich mir. Auch wenn ich keine systematische und strukturierte Arbeit über das IuK-Strafrecht schaffen wollte, weil das vermessen und wegen der vielen Varianten ausgeschlossen wäre, habe ich die Aufgabe unterschätzt. Einige Textteile standen bereits zur Verfügung und mussten nur überarbeitet werden. An anderen Stellen brauchte ich für eine halbe Spalte mehr als zwei Stunden, bis ich die Quellen gefunden und bewertet hatte und mit dem Text endlich zufrieden war. Das erklärt auch einige Längen und Umwege, die der Text aufzuweisen scheint. Im Detail musste ich immer wieder auch nachrangige Fragen ansprechen und lösen, bis ich zu den Problemen in den Überschriften zurückkehren konnte.

Nach zwei Monaten Arbeit an dem Text stelle ich Ihnen das Ergebnis mit 116 Seiten und knapp 50.000 Wörtern, 31 Grafiken und 8 Tabellen vor. Mehr als bei den übrigen Arbeitspapieren erwarte ich Diskussionen, Widersprüche und Hinweise auf misslungene oder unvollständige Auseinandersetzungen. Das ist dem breiten Thema im Neuland geschuldet und unvermeidbar.

Dieter@Kochheim.de

Hannover, im Oktober 2011

1. Internetkriminalität. Was ist das? [11]

> *Internetkriminalität sind Straftaten, die auf dem Internet basieren oder mit den Techniken des Internets geschehen.* Wikipedia

Die Beantwortung der einfach anmutenden Frage ist nicht ganz einfach. Das beginnt schon damit, dass die Internetkriminalität einen Teil der enger gefassten Computerkriminalität umfasst, die schließlich um den Aspekt der globalen Vernetzung erweitert ist. Hinzu kommt die Frage nach dem originären Technikeinsatz (<Technik>kriminalität im engeren Sinne) oder der nur anlässliche Technikeinsatz (... im weiteren Sinne). Besser scheint es, insgesamt von IuK-Kriminalität zu sprechen, die die Informations- und Kommunikationstechnik zusammen fasst und damit den tatsächlichen Verhältnissen am nächsten kommt.

Für die Strafverfolgung spielt die Frage nach dem tatsächlichen Täterhandeln eine erhebliche Rolle, weil davon nicht nur die Anwendung des richtigen materiellen Rechts, sondern auch die staatsanwaltschaftliche und gerichtliche Zuständigkeit abhängt. Spätestens dabei befinden wir uns tief im Verfassungsrecht, weil es auch um den "gesetzlichen Richter" geht (Art 101 Abs. 1 S. 2 GG).

"Computer" ist im engeren Sinne ein isoliertes, also unvernetztes informationsverarbeitendes System, das zum Erstellen, Bearbeiten, Verwalten und Speichern digitaler Dateien jeder Art geeignet und bestimmt ist. Durch ihre Vernetzung werden die Computer zu Telekommunikationsanlagen, wobei die Telekommunikation der technische Vorgang des Aussendens, Übermittelns und Empfangens von Signalen ist (§ 3 Nr. 22 TKG). Im Zusammenhang mit der Onlinedurchsuchung spricht das BVerfG auch von der "Fernkommunikation", die es in den Zusammenhang mit dem Internet stellt [12]. Das lässt vermuten, dass es auch eine "Nahkommunikation" gibt, über die uns das höchste Gericht aber in Unkenntnis lässt.

In der Tat gibt es sie, die Nahkommunikation. Sie beginnt bei der einfachen Peripherie (Tastatur, Scanner, mobile und vernetzte Festplatten), führt über jede Menge Schnittstellen (Bluetooth, Infrarot, Mobilfunk) bis hin zu Heimnetzen und Servern in Firmennetzen. In der Informationstechnik spricht man insoweit von einem Local Area Network - LAN. Es ist ein gekapseltes Netz, das idealer Weise nur über eine Schnittstelle zu weiträumigen Rechnerverbünden verfügt. Aufgrund der heute geläufigen Techniken macht es deshalb Sinn, als "Computer" auch ein lokal begrenztes Verbundsystem anzusehen, das unter einer einheitlichen Verwaltung und Verantwortung steht, also ein LAN ist.

Der Begriff "Telekommunikation" hilft zur Klärung auch nicht weiter. Er ist zwar ursprünglich ein Synonym für das "Fernmeldewesen" gewesen, wird aber sowohl von § 3 Nr. 22 TKG als auch von der gerichtlichen Spruchpraxis erheblich weiter gefasst und meint jede Form der elektromagnetischen Signalverarbeitung. Andererseits schränkt das TKG wieder ein, indem es den Endnutzer als eine Person definiert, die keine öffentlichen Netze oder Dienste betreibt (§ 3 Nr. 8 TKG). Damit wären wir wieder beim gekapselten LAN, in dem dennoch Telekommunikation stattfinden kann - jedenfalls im technischen und verfassungsrechtlichen Sinne.

Das Internet ist ein Wide Area Network - WAN - und auf jedem Fall ein Fernkommunikationsnetz. Nicht jedes WAN ist global, was die Firmennetze internationaler Unternehmen oder der öffentlichen Verwaltung zeigen. Sie kennen geschlossene Verbünde (Virtual Private Network – VPN, Overlay-Netze [13]) und Substrukturen. Von außen betrachtet ist zum Beispiel das niedersächsische Landesnetz

---

[11] Die blau gefärbten Texte (mit Ausnahme der Überschriften) sind mit Links zu den Quellen im Internet unterlegt.

Wörtliche Zitate werden in Kursivschrift und ohne Anführungszeichen wiedergegeben.

[12] **BVerfG**, Urteil vom 27.02.2008 - 1 BvR 370/07, 595/07, Rn 176

[13] **CF**, Overlay-Netze der öffentlichen Verwaltung, 30.03.2008

Die Informations- und Kommunikationstechnik umfasst die Schaffung, Verarbeitung, Speicherung und Vermittlung von elektromagnetische Daten unter Einsatz von Elektrotechnik und ungeachtet der physikalischen Trägermedien und räumlichen Entfernungen. Kochheim

ein Endnutzer, der seinerseits ein gekapseltes und selbstverantwortetes Netz verwaltet. Innerhalb dieses Netzes betreiben große Ressorts jedoch eigene Overlay-Netze, die jedenfalls auf Protokoll- und Zugriffsebene voneinander getrennt sind. Ihre Komponenten sind isoliert, aber räumlich über dieselbe Fläche verteilt. Bei solchen Konstruktionen versagen auf räumliche Distanzen bezogene Definitionen wie das WAN oder das regionale Metropolitan Area Network - MAN. Nur das LAN lässt sich durch eine einheitliche Verantwortung des Betreibers definieren, so dass jedenfalls die Fernkommunikation zwischen verschiedenen LAN in ihrer Rolle als Endnutzer stattfindet (was auch nicht alle Definitionsprobleme löst).

Das zeigt, dass schon eine treffende Differenzierung zwischen "Computer-" und "Internet"kriminalität scheitert. Deshalb ist es notwendig, beide als Formen der Kriminalität im Zusammenhang mit der Informations- und Kommunikationstechnik zusammen zu fassen.

Im Zusammenhang mit der IT-Kriminalität, die nach der allgemeinen Vernetzung nichts anderes als IuK-Kriminalität ist, wurde die Unterscheidung zwischen der speziellen Kriminalität im engeren und weiteren Sinne entwickelt. Das bleibt weiterhin sinnvoll.

Danach handelt es sich um IuK-Kriminalität im engeren Sinne bei den Erscheinungsformen, die unter unmittelbarer Nutzung und Missbrauch dieser Technik erfolgen [14]. Hierfür stehen vor allem solche Begriffe wie Hacking [15], Malware [16] und Botnetze [17].

[14] **CF**, Einleitung. Was sind IT-Straftaten?, 2007

[15] **CF**, Eine kurze Geschichte der Cybercrime, 03.11.2010

[16] **CF**, Malware, 12.05.2008

[17] **CF**, Botnetze, 2007. Siehe auch: Dieter **Kochheim**, Cybercrime, 24.05.2010.

Die IuK-Kriminalität im weiteren Sinne nutzt diese Techniken bewusst, um Straftaten zu begehen, die für sich betrachtet keine IuK-Straftaten sind. Das gilt zum Beispiel für die Beleidigung (§ 185 StGB), die Erpressung (§ 253 StGB), den Betrug (§ 263 StGB) und viele andere mehr (siehe <oben>).

Die Massenerscheinungen sind meistens Formen des Betruges und deshalb IuK-Kriminalität im weiteren Sinne. Dabei missbrauchen die Täter häufig die Technik auf hintersinnige und intelligente Weise, so dass die Ermittler besonderes, auch technisches Wissen brauchen, um sie als Kriminalität zu erkennen, ihre Abläufe zu verstehen und sich auf die Handlungselemente zu konzentrieren, die den strafrechtlichen Gehalt ausmachen. Bei diesen Formen kommt es weniger darauf an, das tatvollendende Handeln wegen seines IuK-Gehaltes zu verstehen und zu bewerten, sondern darauf, den Tatplan und das in ihm liegende Unrecht zu begreifen.

Aus den Zuständigkeitsregeln für die Wirtschaftsstrafsachen ist dieses sachliche Problem bekannt. Neben Wirtschaftsmaterien im engeren Sinne (§ 74c Abs. 1 Nr. 1 bis 5a GVG) sind Wirtschaftsstrafsachen aus dem Vermögensstrafrecht auch solche, bei denen zur Beurteilung des Falles besondere Kenntnisse des Wirtschaftslebens erforderlich sind (§ 74c Abs. 1 Nr. 6 GVG).

Schon wegen der Zuständigkeit stellt sich die Fra-

ge nach den geforderten besonderen Kenntnissen in allen Bereichen der Strafverfolgung. Die erfolgreiche Weichenstellung, die aus den Wirtschaftsstrafsachen überliefert ist, empfiehlt dieses Modell auch für die IuK-Strafsachen, obwohl sie keine saubere Trennschärfe verspricht. Interne Streite mit kreativen Argumentationen sind vorprogrammiert.

Im staatsanwaltschaftlichen Bereich fühlt sich noch niemand so richtig zuständig für die IuK-Strafsachen. Die Wirtschaftsstrafsachen umfassen zwar auch den Computerbetrug, aber nur, wenn zu seiner Beurteilung besondere Kenntnisse des Wirtschaftslebens erforderlich sind. Die Organisierte Kriminalität [18] umfasst zwar ausdrücklich auch den Einsatz moderner, unüblicher Tatwerkzeuge, verlangt aber immer nach den besonderen Indikatoren (Nr. 2.1 Anlage E zu den RiStBV). Die Kenntnis davon ist wenig verbreitet.

Fachabteilungen für IuK-Strafsachen müssen einen definierten Platz erst noch erlangen. Sie müssen sich auf die IuK-Kriminalität im engeren Sinne sowie auf die im weiteren Sinne konzentrieren, wenn zu ihrem Verständnis wirklich besondere Kenntnisse über die Informationstechnik, ihre Abläufe oder soziologischen Hintergründe erforderlich sind. Die Tatsache, dass IuK-Täter auch Mal eine E-Mail schicken, SMS versenden, telefonieren oder gar twittern, ist eine schlichte sozialadäquate Nutzung der Kommunikationstechnik und rechtfertigt jedenfalls keine Spezialzuständigkeit. Nichts gefährdet Fachleute mehr als permanente Abwehrkämpfe oder die Überlastung mit tumben Fleißaufgaben. Dazu sind sie zu schade. Sie müssen sich immer wieder in neue Materien und Problemfelder einarbeiten, eindenken und Lösungen entwickeln, die nicht immer strukturiert und statistikkonform abgearbeitet werden können. Das erfordert Zeit, führt zwangsläufig zu ineffektiven Umwegen und vorübergehenden Fehlern und ist der einzige Weg, um Neuländer zu beherrschen. Wer diese Prozesse mit der Stoppuhr begleitet, gehört nicht nur geohrfeigt.

Staatsanwaltschaftliche Zuständigkeitsprüfung:

Bin ich zuständig?

Bin ich wirklich zuständig?

Kann das nicht wer anderes machen?

Besonderer Syllogismus:

Ich bin Allgemeindezernent. Das kann ich nicht!

Meint: Einerseits habe ich viel zu tun und andererseits will ich pünktlich Feierabend machen. Um den Scheiß kann ich mich nicht auch noch kümmern. Im Zweifel bleibt er liegen.

Ich bin jetzt 60 Jahre alt. Das verstehe ich nicht mehr.

Meint: Ich fühle mich seit 30 Jahren unverändert wie 60 Jahre alt. Um das Verständnis, um das ich mich schon immer gedrückt habe, muss ich mich jetzt auch nicht mehr kümmern.

Das ist eine Bande, also ist das Organisierte Kriminalität.

Meint: Ich kann bis drei zählen. Wenn zwei Täter aus den alten Ostblockstaaten kommen, dann haben sie sicherlich einen Residenten vor Ort und dann sind sie eine Bande und dann sind sie auch organisiert.

Das versteht auf Anhieb nur der Kochheim. Der macht das!

Homage an meine Behördenleitung. Oder: Was scheren mich formelle Zuständigkeiten?

[18] **CF**, Organisierte Kriminalität, Vereinigung, Bande, 2007

1.1 IuK-Straftaten im engeren Sinne

Das IuK-Strafrecht im engeren Sinne besteht aus vier Hauptgruppen, die über das Strafgesetzbuch verteilt sind (siehe auch die Übersicht auf der nächsten Seite [19]). Folgende Hauptgruppen habe ich 2007 benannt [20]:

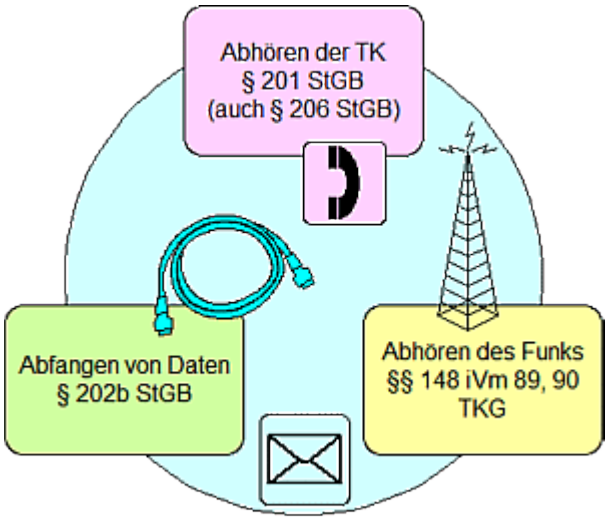
- Computersabotage
- persönlicher Lebens- und Geheimbereich
- Schutz des Rechtsverkehrs
- strafbare Vorbereitungshandlungen

Das IuK-Strafrecht bildet keine geschlossene Gruppe, sondern ist in andere Abschnitte des StGB eingebunden. Zusammen gehalten wird es von der gemeinsamen Definition von Daten in § 202a Abs. 2 StGB:

Daten ... sind nur solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden.

Die Grundtatbestände des IuK-Strafrechts im engeren Sinne sind ganz überwiegend in dem Bereich der einfachen und mittleren Kriminalität angesiedelt worden [21]. Das Abfangen von Daten (§ 202b StGB), die Datenveränderung (§ 303a StGB) und der Funkschutz (§ 148 TKG) drohen mit einer Höchststrafe von 2 Jahren Freiheitsstrafe, das allgemeine Abhörverbot (§ 201 StGB), das Ausspähen von Daten (§ 202a StGB) und die Computersabotage (§ 303b StGB) mit Freiheitsstrafen bis zu 3 Jahren.

Den oberen Bereich der mittleren Kriminalität decken der Computerbetrug (§ 263a StGB), die Fälschung beweiserheblicher Daten (§§ 269, 270 StGB) und die beiden Qualifikationsformen des qualifizierten Abhörverbots beim Amtsträger (§ 201 Abs. 3 StGB) und der schweren Computersabotage ab (§ 303b Abs. 2 StGB), die im Höchstmaß mit Freiheitsstrafen von fünf Jahren drohen.



Zur schweren Kriminalität mit ihren Strafdrohungen von sechs Monaten im Mindest- und bis zu zehn Jahren im Höchstmaß zählen schließlich die besonders schweren Computerbetruge (§§ 263a Abs. 2, 263 Abs. 3 StGB), Computersabotagen (§ 303b Abs. 4 StGB) und Fälschungen beweiserheblicher Daten (§§ 269 Abs. 3, 267 Abs. 3 StGB). Die schärfsten Strafdrohungen bestehen wegen des gewerbsmäßigen Bandencomputerbetruges (§§ 263a Abs. 2, 263 Abs. 5 StGB) und der gewerbs- und bandenmäßigen Fälschung beweiserheblicher Daten (§§ 269 Abs. 3, 267 Abs. 4 StGB), die als qualifizierte und damit selbständige Verbrechen mit Freiheitsstrafen zwischen einem und zehn Jahren drohen.

Die strafbaren Vorbereitungshandlungen [22] im IuK-Strafrecht im engeren Sinne sind ausnahmslos mit einer Höchststrafe von einem Jahr Freiheitsstrafe bedroht und damit im Bereich der leichten Kriminalität angesiedelt. Ihre zentrale Vorschrift ist der § 202c StGB. Ihre gesetzessystematische Einordnung ist schlecht gelungen, weil der Wortlaut den Eindruck erweckt, die illegalen Vorbereitungen würden sich nur auf das Abfangen und Ausspähen von Daten beziehen [23]. Das

---

[19] Die Übersicht stammt aus dem Jahr 2010: **CF**, am Ende kommt der Cyberwar, 22.08.2010.

[20] **CF**, IT-Strafrecht, 2007. Der vier Jahre alte Text hat an Aktualität kaum eingebüßt und wurde hier aktualisiert und übernommen.

[21] Siehe Schaubild auf Seite 5.

[22] **CF**, Vorbereitung: Ausspähen, Abfangen und Sabotage, 2007

[23] Das BVerfG weiß bei seiner Entscheidung zum Hackerstrafrecht davon, wählt dann aber eine missverständliche Formulierung: *Tatobjekt des § 202c Abs. 1 Nr. 2 StGB kann nur ein Programm sein, dessen Zweck die Begehung einer Straftat nach §*

Betrug und Untreue	Programme	§ 263a Abs. 3 StGB
Funkschutz	Abhörverbot	§§ 148 Abs. 1 Nr. 1, 89 TKG
Geld- und Wertzeichenfälschung	Programme, Vorrichtungen	§ 149 StGB
gemeingefährliche Straftaten	TK-Einrichtungen	§ 317 StGB
persönlicher Lebens- und Geheimbereich	Ausspähen	§ 202a StGB
	Abfangen	§ 202b StGB
	Hackerparagraph	§ 202c StGB
	Fernmeldegeheimnis	§ 206 StGB
Sachbeschädigung	Datenveränderung	§ 303a StGB
	Computersabotage	§ 303b StGB
sexuelle Selbstbestimmung	Kinderpornographie	§ 184b StGB
Urheberrecht	Kopierschutz	§ 108b UrhG
Urkundenfälschung	technische Aufzeichnungen	§ 268 StGB
	beweiserhebliche Daten	§ 269 StGB
	Datenverarbeitung	§ 270 StGB
Wettbewerbsrecht	Geschäftsgeheimnis	§ 17 UWG

stimmt aber nicht, weil auch die Datenveränderung (§ 303a Abs. 3 StGB) und die Computersabotage (§ 303b Abs. 5 StGB) auf den § 202c StGB "rück"verweisen, ohne dass sich das in dieser Strafnorm spiegelt [24].

Mit der Reform von 2007 hat der Gesetzgeber alle Formen der elektronischen Kommunikation abdecken und noch vorhandene Lücken schließen wollen [25]. Das ist ihm nicht gelungen, was eine Reihe von Lücken im Detail und vor allem der Funkschutz beweisen, weil er das Abhören des Funks für die Frequenzen des Amateurfunks nicht verbietet [26]. Die IT-spezifischen Frequenzbänder für drahtlose Netze und den Nahfunk liegen überwiegend in den Frequenzbereichen, die dem Amateurfunk zugewiesen sind.

1.2 Erscheinungsformen und Tatbestände

Von klassischen Strafnormen ist man gewohnt, dass sie unmittelbar auf die Erscheinungsformen der Kriminalität ansprechen. Wer fremde Sachen kaputt macht (§ 303 StGB) oder klaut (§ 242 StGB), andere körperlich verletzt (§ 223 StGB) oder tötet (§ 212 StGB), wird bestraft. Viele Strafvorschriften scheinen deshalb direkt aus den Zehn Geboten zu entstammen und sie allenfalls wegen ihrer Einzelheiten auszugestalten, was wahrscheinlich sogar stimmt [27].

Eine Strafvorschrift nach dem Motto, Du darfst nicht hacken, keine Malware programmieren, verbreiten oder einsetzen oder Du darfst keine Botnetze betreiben, wird man nicht finden. Mit dem Computerbetrug (§ 263a StGB) hat der Gesetzgeber hingegen eine solide Lösung gefunden, weil sie alle vermögensrelevanten, auf Technik fußenden Manipulationen erfasst. Wegen anderer einschlägiger Strafvorschriften ist dieser Weitblick nicht erkennbar. Eine Vorschrift gegen die Datenhehlerei fehlt ganz. Einen Teil davon deckt § 17

202a StGB (Ausspähen von Daten) oder § 202b StGB (Abfangen von Daten) ist.
BVerfG, Beschluss vom 18.05.2009 – 2 BvR 2233/07, Rn 60.

24 **CF**, vorverlagertes Hackerstrafrecht, 04.09.2008

25 **CF**, Schutz der Kommunikation, 2007

26 Ebenda, Abgrenzungen, 2007

27 Präambel zum GG: *Im Bewußtsein seiner Verantwortung vor Gott und den Menschen ...*

UWG wegen der Geschäftsgeheimnisse ab und mit einer gewissen Hilflosigkeit wird gelegentlich das Datenschutzrecht bemüht [28]. Mit § 44 BDSG droht es eine Höchstfreiheitsstrafe von zwei Jahren an, wobei die Strafverfolgung unter dem Vorbehalt eines Strafantrages steht, der noch nicht einmal durch ein besonderes öffentliches Interesse an der Strafverfolgung ersetzt werden kann. Aufgrund seines allgemeinen Charakters wird es von jeder speziellen Vorschrift und vor allem von solchen mit höherer Strafdrohung verdrängt.

Die Erfahrungen lehren, dass die IuK-Kriminalität in den meisten Fällen mehraktig ausgeführt wird, so dass zu ihrer Erfassung nicht nur ihre öffentliche Erscheinungsform betrachtet werden darf. Sie offenbart häufig nur einen Ausschnitt von dem Tatplan und seinen Ausführungsschritten und vielfach zeigen erst die unsichtbaren Folgeschritte den strafrechtlichen Gehalt und die richtige materiellrechtliche Zuordnung. Das zeigen die anschließenden Beispiele.

Diese Erfahrungen lehren auch, dass bei der Strafverfolgung nicht nur wegen der tatsächlichen Zusammenhänge Neuland betreten wird, sondern in aller Regel auch wegen der Rechtsfragen, die mit der IuK-Kriminalität verbunden sind. Darauf bin ich unlängst wegen der Verfahrensfragen eingegangen [29]. Das gilt besonders aber für die Fragen nach der materiellen Strafbarkeit, die ich bislang im Interesse der Beschreibung von Erscheinungsformen und Strukturen der Cybercrime sowie ihren Varianten zunächst zurückgestellt habe [30].

Nur mit der Erscheinungsform des Skimmings habe ich mich tiefer beschäftigt und dafür Anerkennung bekommen [31]. Dazu musste ich mir nicht nur die Grundlagen für den bargeldlosen Zahlungsverkehr erarbeiten, sondern auch tief in die Grundfragen des Allgemeinen Teil des Strafgesetzbuches (Täterschaft, Versuch ua) und zur Bande einsteigen. Mir persönlich hat das dazu verholfen, mich auf den aktuellen Stand der Rechtsprechung zu bringen.

[28] Zuletzt wegen des Skimmings: Alexander **Seidl**, Katharina **Fuchs**, Zur Strafbarkeit des sog. "Skimmings", hrr-strafrecht.de 6/2011, S. 265.

[29] Dieter **Kochheim**, Verdeckte Ermittlungen im Internet, 27.07.2011

[30] Aufsätze zur Cybercrime, 10.08.2011

[31] Arbeitspapier Skimming

2. Materielles IuK-Strafrecht

Die folgenden Beschreibungen von Fallgruppen und ihre materiellrechtliche Bewertung ersetzen keine systematische Aufarbeitung oder Kommentierung. Das wäre vermessen und angesichts der Vielzahl von Varianten kaum möglich. Statt dessen stellen sie die Frage, was bei einer IuK-Straftat tatsächlich geschieht, um dann die richtigen Vorschriften auf sie anzuwenden.

Das IuK-Strafrecht ist anspruchsvoll, aber auch nicht anspruchsvoller als andere besondere Rechtsgebiete. Die folgenden Erörterungen beschäftigen sich mit den Standardfragen im Zusammenhang mit der Cybercrime. Sie gehen nur gelegentlich in die Verästelungen und befassen sich vor allem mit den strukturellen Fragen, die sich aufgrund einer Gesamtschau auf die Erscheinungsform eröffnen. Sie zeigen unerwartete Lösungen und Probleme, die bei einer kleingliedrigen Betrachtung einzelner Erscheinungsformen verschlossen bleiben würden.

Dabei lasse ich alle Fragen aus, die mit grenzüberschreitenden Ermittlungen und der Verfolgung von Straftaten zu tun haben, die vollständig oder teilweise im Ausland begangen werden. Sie müssen einer künftigen Betrachtung vorbehalten bleiben und sind auch – zunächst – unwichtig, weil es in erster Linie darauf ankommt, die materielle Strafbarkeit nach nationalem Recht zu betrachten. Erst wenn insoweit Klarheit über die Strafbarkeit als solche und die Schwere der betroffenen Kriminalität besteht, lässt sich auch die internationale Geltung sinnvoll beurteilen. In vielen Fällen zeigt sich, dass jedenfalls die materielle Strafbarkeit auch im Inland gegeben ist und nur die Ermittlungshandlungen an hoheitlichen Grenzen scheitern.

2.1 Skimming

Die öffentliche Aufmerksamkeit hat das Skimming dadurch erlangt, dass verschiedene Täter entweder beim Abgreifen der Magnetstreifendaten und PIN (Skimming im engeren Sinne) oder beim Einsatz gefälschter Zahlungskarten (Cashing) beobachtet und ergriffen wurden. Beim Abgreifen kommen technische Geräte zum Einsatz, Kartenlesegeräte (Skimmer), die im oder am Karteneinzugsschacht installiert werden, und PIN-Skimmer in Form von Kameras, mit denen die Tastatureingaben beobachtet werden, oder handwerklich häufig hervorragend gearbeitete Tastaturaufsätze.

Das öffentliche Auftreten der Täter und die handwerklichen Fähigkeiten, die von ihnen verlangt werden, haben mich lange daran zweifeln lassen, ob das Skimming wirklich ein Teil der IuK-Kriminalität ist. Der hemmungslose Handel mit dem Equipment und den abgegriffenen Daten in den Hackerboards und die deutliche Durchmischung der Skimming- und der übrigen Cybercrime-Szene haben mich schließlich überzeugt. Hinzu kommt, dass sich die Methoden der Datenbeschaffung erweitert haben und elektronische Direktabgriffe an Geldautomaten [32] sowie Hacking-Angriffe gegen Finanzdienstleistungsunternehmen gemeldet wurden, wobei die Daten direkt manipuliert und gestohlen wurden [33].

Betrachtet man das Skimming im engeren Sinne und konzentriert sich auf die Datenbeschaffung, dann denkt man zunächst an das Ausspähen von Daten oder andere Delikte, die sich mit der Datenintegrität befassen. Erst der Blick auf die Folgeakte des Tatplans eröffnet die materielle Dimension. In der Vorstellung der Täter ist das Abgreifen ein unverzichtbarer Teil des Tatplans, der das finale Cashing überhaupt erst möglich macht. Für sich betrachtet sind die abgegriffenen Daten wertlos, wenn sie nicht weiterverkauft oder von Komplizen eingesetzt werden. Das Cashing verlangt nach gefälschten Zahlungskarten und das bedeutet, dass zwischen dem Abgreifen und dem Cashing

---

[32] Arbeitspapier Skimming

[33] **CF**, Skimming an der Quelle, 20.03.2009

falsche Zahlungskarten hergestellt werden müssen.

Das Herstellen, Sichverschaffen und der Gebrauch gefälschter Zahlungskarten mit Garantiefunktion ist ein Verbrechen, das der Fälschung von Geld gleichgestellt ist (§§ 152a, 152b StGB). Auf arbeitsteilige Tätergruppen hat das verschiedene Auswirkungen. Den Fälschern und Cashern drohen mindestens ein oder zwei Jahre Freiheitsstrafe, je nach dem, ob sie auch als Bande oder gewerbsmäßig handeln (§152b Abs. 2 StGB). In aller Regel handeln die "Abgreifer" als Mittäter der Casher und müssen sich deren Taterfolg zurechnen lassen (§ 25 Abs. 2 StGB), wobei sie sich bereits an dem Versuch der Fälschung beteiligen können, sobald sie die abgegriffenen Daten an ihre Komplizen übermitteln [34]. Schon davor beteiligen sie sich in einer besonderen Form an dem Fälschungsverbrechen, weil bereits dessen verbindliche Verabredung zwischen Mittätern strafbar ist (Verabredung zu einem Verbrechen, § 30 Abs. 2 StGB).

Das Skimming im engeren Sinne ist deshalb weniger eine abgeschlossene Tat für sich, sondern eine strafbare Vorbereitungshandlung zum Fälschen und Gebrauchen von Zahlungskarten mit Garantiefunktion [35], wobei beim Cashing gleichzeitig ein Computerbetrug begangen wird [36] (§ 152b StGB in Tateinheit mit § 263a StGB). In dem Vorbereitungsstadium können noch andere Strafvorschriften zum Zuge kommen, vor allem § 149 StGB wegen des Umgangs mit Skimmern und § 263a Abs. 3 StGB wegen der für das PIN-Skimming präparierten Kameras und Tastaturaufsätze, nicht aber die Strafvorschrift über das Ausspähen von Daten selber (§ 202a StGB [37]), an die jeder zuerst denkt.

Die Einzelheiten müssen teilweise noch differenzierter betrachtet werden als in diesem Überblick. Sie werden in dem Arbeitspapier Skimming erörtert [38].

2.1.1 Cash Trapping

Auch das klassische Front Covering, bei dem die gesamte Fassade eines Geldautomaten mit einer Attrappe abgedeckt wird, erlebt seit einem Jahr mit dem „Cash Trapping“ eine Wiedergeburt: Mit einer Blende wird einfach nur der Geldausgabeschacht überdeckt, so dass die Geldscheine in den Zwischenraum hinter der Blende rutschten, wo sie mit Klebstoff „festgehalten“ werden. Sobald die enttäuschten Bankkunden die Filiale verlassen haben, können die Täter die Geldscheine in Ruhe bergen. Das erfordert eine ständige Beobachtung des Geldautomaten und bringt nicht den beachtlichen Gewinn von durchschnittlich etwa 2.350 Euro je gefälschter Karte [39], die beim Cashing erzielt werden [40]. Die Methode hat jedoch den Vorteil, dass die Täter die Beute sofort erzielen.

Die rechtliche Beurteilung dieses Vorgehens ist noch streitig. Ich betrachte das „Cash Trapping“ als einen „normalen“ Diebstahl (§ 242 StGB). Diskutiert werden aber auch Betrug (§ 263 StGB) und Unterschlagung (§ 246 StGB). Ein Betrug ließe sich dann annehmen, wenn man eine Vermögensverfügung des „entnervten“ Bankkunden darin sieht, dass er auf den Besitzerwerb am vom Automaten ausgegebenen Geld verzichtet. Das ist aber kein bewusster Akt, weil ihm nicht bekannt ist, dass sich das Geld hinter der aufgesetzten Blende befindet. Eine Unterschlagung scheitert daran, dass der Täter zu keinem Zeitpunkt einen rechtmäßigen Gewahrsam an dem ausgegebenen Geld erlangt.

---

[34] **BGH**, Urteil vom 27.01.2011 - 4 StR 338/10

[35] Mit fast den gleichen Worten argumentiert jetzt der **BGH**, Beschluss vom 11.08.2011 - 2 StR 91/11, Rn 9.

[36] **BGH** ebenda, Rn 13.

[37] **BGH**, Beschluss vom 18.03.2010 - 4 StR 555/09

[38] Dieter **Kochheim**, Skimming. Hintergründe und Strafrecht, 22.04.2011

[39] Eigene Berechnung anhand der für 2009 veröffentlichten Zahlen.

[40] Gebrauch von gefälschten Zahlungskarten mit Garantiefunktion beim Skimming.

2.1.2 Regelungslücken

Dadurch, dass der Gesetzgeber das Skimming in das Geldfälschungsrecht eingebunden hat, hat diese Kriminalitätsform umfangreiche Ausprägungen auch an anderen Stellen erfahren. Das zeigt sich zum Beispiel daran, dass es dem Weltrechtsprinzip unterworfen ist (§ 6 Nr. 7 StGB), so dass auch reine Auslandstaten im Inland strafbar sind. Sogar die unbeteiligten Mitwisser werden von § 138 Abs. 1 Nr. 4 StGB mit Strafe wegen der Nichtanzeige geplanter Straftaten bedroht. Schließlich unterfällt schon der Umgang mit Skimmern der Strafbarkeit gemäß § 149 StGB und zu guter Letzt ist er auch eine Ordnungswidrigkeit gemäß § 127 OWiG.

Das gilt jedoch nur wegen des „Fälschungsanteils“ beim Skimming und nicht wegen des Computerbetruges, der beim Gebrauchen der gefälschten Zahlungskarten ebenfalls begangen wird (§ 263a StGB). Das Abgreifen der PIN hat nichts mit dem Fälschen zu tun und dient allein dazu, beim Cashing erfolgreich den Computerbetrug auszuführen.

Das hat zur Folge, dass die PIN-Skimmer nach ganz anderen Lösungen verlangen als die Kartenlesegeräte, weil sie nicht dem § 149 StGB unterfallen. § 263a Abs. 3 StGB kennt einen eigenen Gefährdungstatbestand im Vorbereitungsstadium, der sich aber auf den Umgang mit „Computerprogrammen“ beschränkt, die für den Computerbetrug entwickelt werden. Damit ist der Umgang mit Hardware für sich alleine nicht strafbar, auch wenn zum Beispiel Handys in Attrappen eingebaut oder sie mit weiteren Akkus verlötet werden, ohne dass auch ihre elektronische Steuerung manipuliert oder ersetzt wird (Dual Use) [41].

Wegen des Ausspähens der PIN kann für sich allein betrachtet eine strafrechtliche Haftung im Erfolgsfall aus § 303b Abs. 5 in Verbindung mit § 202c StGB abgeleitet werden. Diese Rechtsfolge erschließt sich jedoch nur dem, der sich im Strafgesetzbuch auskennt und auch noch die richtigen Schlüsse zieht.

Die notwendige Unterscheidungen zwischen Magnetstreifen-Skimmer, PIN-Skimmer mit eigenständigem Programm oder auf der Basis von Dual Use, verschiedene Haftungsgrundlagen während des Skimmings im engeren Sinne bis hin zum Beginn des Versuchs bei der Übermittlung der ausgespähten Daten an die Hinterleute, der nicht auch den Beginn des Versuchs wegen des Computerbetruges auslöst, verlangen von der Strafverfolgung die Betrachtung verschiedener Handlungsschwerpunkte und Tatabläufe, die die Ermittlungen und schließlich das abschließende Urteil erheblich erschweren.

Das liegt besonders daran, dass das Skimming im engeren Sinne keine eigene Strafnorm hat, sondern als Gefährdungsdelikt im Vorbereitungsstadium zum Fälschen angesiedelt ist. Die Normen des IuK-Strafrechts geizen nicht mit Strafvorschriften für das Vorbereitungsstadium, lassen aber eine sinnige Struktur und klare Linien vermissen. Das gilt besonders für die Beschränkung auf die „Computerprogramme“ in § 263a Abs. 3 StGB und die „Passwörter oder sonstige Sicherungscodes“ in § 202c Abs. 1 Nr. 1 StGB unter Ausschluss aller Formen von Hardware. Auch § 149 Abs. 1 Nr. 1 StGB lässt die rechte Wortklarheit vermissen, weil die Strafbarkeit des Umgangs mit Skimmern aus den Worten „Computerprogramme oder ähnliche Vorrichtungen“ abgeleitet werden muss.

Das lässt eine klare Zusammenfassung aller Gefährdungstatbestände wünschen, die auf absehbare Zeit nicht zu erwarten ist.

---

[41] In Rauchmelder eingebaute Handys oder andere Attrappen können zwar nicht als Beziehungsgegenstände sichergestellt werden, wohl aber als Beweismittel, die die Vorbereitung und Verabredung eines Verbrechens unterstreichen.

2.2 Rückruftrick

Mit der digitalen Telefonie unter dem ISDN-Protokoll [42] wurden seit 1995 intelligente Telefonnetze in aller Breite möglich, in denen besondere Angebote wie Mehrwert-, Auskunfts- und Dienste mit Kostenteilung angeboten werden konnten [43]. Sie haben dazu geführt, dass telefonische und andere Kommunikationsdienste im Zusammenhang mit dem Internet miteinander verwachsen sind und sich vor allem nur noch durch ihre Protokolle unterscheiden (Konvergenz). Der Rückruftrick konzentriert sich auf den Missbrauch von Mehrwertdiensten und hat damit einen festen Platz in der IuK-Kriminalität im weiteren Sinne.

2.2.1 Mehrwertdienste und Regulierung

Hinter den Mehrwertdiensten (auch: Premium Rate) steckt die Vorstellung, dass der Zugangsprovider nicht nur eine TK-Verbindung herstellt, sondern *darüber hinaus eine weitere Dienstleistung erbracht wird, die gegenüber dem Anrufer gemeinsam mit der Telekommunikationsdienstleistung abgerechnet wird* [44]. Dafür war zunächst der Nummernkreis (0)190 reserviert, wobei die Rufnummerngasse (0)19 **00** frei tarifierbar war [45]. Dazu bedurfte es nur einer Vereinbarung zwischen dem Zugangsprovider und dem Anschlussinhaber. Schnell folgten Missbräuche von Premium Rate-Diensten, die die betroffenen Kunden mit immensen Kostenforderungen überraschten. Die Methoden waren immer dieselben: Täuschung über die Tatsache, dass ein solcher Dienst angerufen wird, kostenpflichtige Warteschleifen, Schlechtleistung und untergeschobene Dialer [46].

2003 reagierte der Gesetzgeber mit einer erfolgreichen Regulierung [47]. Er schuf den Nummernkreis (0)190 ab, führte dafür den neuen Nummernkreis (0)900 ein, deckelte den dabei abrechnungsfähigen Mehrwertanteil (§ 66d TKG) und führte eine Meldepflicht für Mehrwertdienste und Dialer ein. Dazu wurden bei der Bundesnetzagentur – BNA – drei Datenbanken mit den Betreiberdaten eingerichtet. Bei Missbräuchen kann die BNA Rufnummern entziehen, sperren und den Anschlussinhabern die Rechnungslegung untersagen (§ 67 Abs. 1 TKG). Das hat zur Folge, dass die Betreiber ihre vorgeblichen Forderungen nicht mehr gerichtlich durchsetzen können. Die in § 149 TKG aufgeführten Ordnungswidrigkeiten zeigen die Ferkeleien, die im Zusammenhang mit den Mehrwertdiensten stattgefunden haben und noch immer gelegentlich probiert werden [48]. Dazu werden jetzt häufig teure Auslandsnummern verwendet [49], die keine strikte Regulierung wie hierzulande kennen.

2.2.2 automatisierter Rückruftrick

Eine besonders dreiste Form des Rückruftricks wurde 2002 publik und kann sich jederzeit wiederholen [50]. Der Inhaber von mehreren Mehrwertdienstnummern startete auf seinem Computer ein Programm, das den D1-Nummernkreis systematisch anwählte und die Verbindung sofort wieder unterbrach. Das reichte aber für die Meldung "Anruf in Abwesenheit" auf dem Handy. Nur wenige der Empfänger wählten den Anrufer an und bekamen das Freizeichen zu hören, so als wenn keine Verbindung zustande gekommen wäre. Das Freizeichen stammte jedoch vom Tonband und der Gebührenzähler lief. Sehr lukrativ. Der Täter

---

42 Integrated Services Digital Network - ISDN

43 **CF**, intelligente Nummernverwaltung, 21.11.2008

44 **BNA**, Nummernverwaltung. 0900

45 **CF**, 1900-Nummern. Abrechnung. Missbrauch, 21.11.2008

46 Dialer sind automatische Einwahlhilfen, die vor allem dadurch bekannt geworden sind, dass sie die Internetzugänge von PCs auf teure Mehrwertdienstenummer „umgebogen“ haben. Sie stellen eine frühe Form der Malware dar, auf die noch näher eingegangen wird.

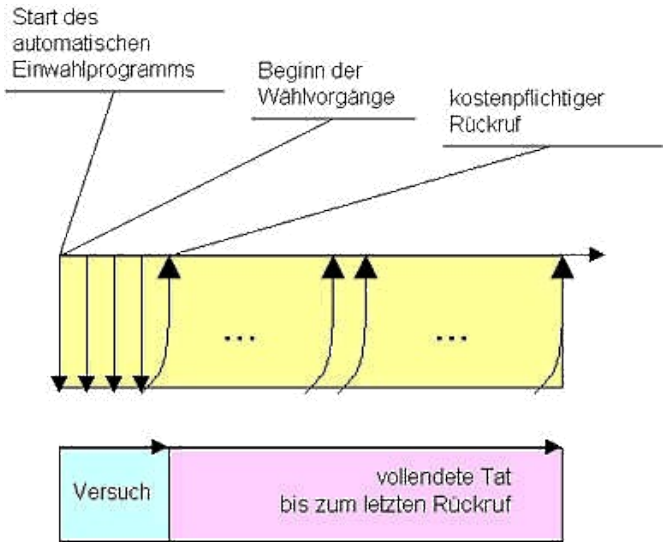
Siehe: **CF**, rechtliche Handhabung, 21.11.2008.

47 Gesetz zur Bekämpfung des Missbrauchs von 0190er-/0900er-Mehrwertdiensterufnummern, 09.08.2003

48 **CF**, Regelungen im TKG, 21.11.2008

49 **CF**, Auslandsvorwahlnummern, 21.11.2008

50 0190-Betrug: Jetzt mit "gefälschten" Freizeichen, Heise online 07.08.2002



wurde später wegen Betruges zu Freiheitsstrafe verurteilt [51].

Materiell handelt es sich tatsächlich um einen Betrug im Sinne von § 263 StGB. Der Täter nutzt zwar die technischen Möglichkeiten, die ihm die mobile Telefonie (Anzeige eines Anrufes in Abwesenheit) und die Computertechnik bieten (automatisches Wählen in Verbindung mit einer Telefonanlage), wählt aber den angesprochenen Nummernkreis selber und startet auch den technischen Vorgang. Dabei hofft er darauf, dass das Opfer unbedacht die Rückruf-Taste seines Handys drückt und dabei nicht vor Augen hat, dass die Verbindung zu einem Mehrwertdienst erfolgt. Das gewählte Beispiel ist deshalb besonders infam, weil die Verbindung tatsächlich aufgebaut und aufrecht erhalten bleibt, während der Anrufer arglos nur ein Freizeichen hört und sich die Gebühren summieren.

Mit dem Start des Einwahlprogramms setzt der Täter nach seiner eigenen Vorstellung von der Tat unmittelbar zur Verwirklichung des Tatbestandes an (Versuch, § 22 StGB). Mit der Auswahl des Nummernkreises hat er die mögliche Zahl und die persönlichen Merkmale der Betroffenen eingegrenzt (Anschlussinhaber unter dem Nummernkreis von D1) und muss keine Handlungen mehr beitragen, um einen Taterfolg herbeizuführen. Alle weiteren Handlungen können nur von dem Opfer selber ausgeführt werden, das mit dem Rückruf den automatischen Gebührenabrechnungsmechanismus anstößt. Der geforderte Irrtum besteht in der Person der Anrufers, der nicht damit rechnet, eine Mehrwertdienstnummer anzurufen, und auch nicht damit, mit einem Tonband oder einem anderen Wiedergabegerät recht einseitig zu kommunizieren. Dabei wird keine technische Einrichtung manipuliert, sondern allein auf die Arglosigkeit des Opfers spekuliert. Dessen Schaden besteht in dem Mehrwertanteil des abgerechneten Entgeltes, der am Ende an den Täter abgeführt wird. Der beträchtliche Technikaufwand, die Einrichtung mehrerer Mehrwertdienstnummern und der auf mehrere Monate ausgerichtete Betrieb der Technik legen einen gewerbsmäßigen Betrug im Sinne von § 263 Abs. 3 Nr. 1 StGB nahe.

Der Tatablauf ist prinzipiell der gleiche, der auch für den Massenversand von Spam- und Phishing-Mails gilt: Der Täter handelt nur ***einmal***, indem er den Versand von Nachrichten startet. Die potentiellen Opfer sind aber breit in der Fläche verstreut. Wenn sie mit einer Verzögerung von mehreren Wochen mit ihrer Telefonrechnung zu ihrer örtlichen Polizei gehen [52], wird die wahrscheinlich den Inhaber der Mehrwertdienstnummer ermitteln und die Akten an die örtlich zuständige Staatsanwaltschaft abgeben.

Der überschaubare Schaden, den der einzelne Anzeigeerstatter erlitten hat, könnte den zuständigen Staatsanwalt dazu veranlassen, das Ermittlungsverfahren gegen eine geringe Geldauflage vorläufig gemäß § 153a StPO einzustellen. Zahlt der Täter die Buße, dann tritt wegen aller anderen Geschädigten Strafklageverbrauch ein (Art 103 Abs. 3 GG [53]), weil alle Schadensereignisse auf das einmalige Handeln des Täters beim Start des Computerprogramms zurück gehen. Sie sind Teil

[51] Die Textpassage stammt aus: **CF**, Rückruftrick, 2007

[52] Ich spreche deshalb häufig von dem „Wäh“, also von dem Menschen, der sich mit seiner Telefonrechnung bewaffnet bei der Polizei über Betrug beschwert.
Zuletzt: **CF**, der "Wäh!", 01.02.2011

[53] Dasselbe gilt für Strafbefehle, sobald sie rechtskräftig, und für Anklagen, sobald sie zur Hauptverhandlung zugelassen sind.

einer einheitlichen prozessualen Tat (§ 264 Abs. 1 StPO).

Das Beispiel lehrt, dass sich auch in Strafanzeigen wegen kleinerer Schäden Teile einer groß angelegten Straftat verbergen können, die nur dann angemessen beurteilt werden kann, wenn ihre Teilakte im Rahmen der Strafverfolgung zusammen geführt werden. Die dazu nötigen Mechanismen, vor allem Melde- und Analysedienste, sind bis heute unvollständig. Allerdings ist die Sensibilität bei den polizeilichen Fachbehörden erheblich gestiegen, so dass jedenfalls erwartet werden kann, dass der klassische Rückruftrick angemessen bearbeitet wird.

2.3 Hacking und Malware

Im Vorgriff auf die besonderen Erscheinungsformen der IuK-Kriminalität müssen die Phänomene und Methoden grundsätzlich betrachtet werden, weil sie in Varianten immer wieder auftauchen.

Noch heute währt eine ideologische Auseinandersetzung über die vor 50 Jahren entstandene Hackerkultur an, wobei sich die Hackerszene von den bedenkenlosen Skript-Kiddies, die unbedacht und skrupellos mit zerstörerischen Werkzeugen hantieren, ohne sie selber entwickelt zu haben oder sie zu beherrschen, von den Crackern, die vor allem Zugangssicherungen zu Programmen und Systemen durchbrechen, um kostenpflichtige Programme oder Dienste ohne Entgelt nutzbar zu machen, und von den Kriminellen abgrenzt, die mit Profitinteresse Malware herstellen, verkaufen und pflegen, Botnetze betreiben, Phishing und andere Formen des Identitätsdiebstahls [54] praktizieren. Darin kommt viel Hilflosigkeit zum Vorschein, weil alle, die „Guten“ wie die „Bösen“, dieselben Methoden, Werkzeuge und Angriffsziele verwenden und sich allenfalls im Motiv unterscheiden. Das zeigt ganz besonders die Auseinandersetzung um das Hackerkollektiv Anonymous [55].

Hacking und Malware stellen die beiden grundlegenden Strategien dar, mit denen die Penetration bei der IuK-Kriminalität betrieben wird. Beim Hacking erfolgt ein individuell gesteuerter Angriff gegen informationsverarbeitende Systeme mit dem Ziel, in sie einzudringen und zu penetrieren. Der nähere Zweck der Einflussnahme orientiert sich an den Motiven des Hackers und kann wegen des technischen Vorgehens offen bleiben.

Die Spannbreite der Akteure und ihrer Motive reicht von berechtigten Auftragsarbeiten von Sicherheitsunternehmen über wohlmeinende, sich aufdrängende Experten bis hin zu Datendieben, Industriespionen und zerstörungswütigen Vanda-

---

[54] Siehe: Identitätsdiebstahl und Phishing, in: Dieter **Kochheim**, Cybercrime, 24.06.2010, S. 45.

[55] **CF**, IT-Söldner im Kampfeinsatz, 15.02.2011; Dieter **Kochheim**, Eskalationen, 20.02.2011.

len (Hacktivismus [56], Defacement [57], Erpressung, kalter Cyberwar [58]).

Tatsächlich ist es geboten, nicht einfach nur von Hackern zu sprechen. Davon gibt es viele und ganz verschiedene. Ihnen ist gemeinsam, dass sie tiefe technische Kenntnisse haben und bereit und in der Lage sind, diese auch praktisch anzuwenden.

▸ Die, die an anderer Stelle als "gute" oder "weiße" Hacker bezeichnet werden, nenne ich wegen ihrer universitären Herkunft die ***akademischen Hacker***. Sie suchen nach technischen Schwachstellen sowie anderen Schwächen in der IT-Organisation und entwickeln sogar Lösungen, um mehr Sicherheit zu schaffen. Sie verursachen keine böswilligen Schäden, allenfalls unbedachte Flurschäden, streben nicht nach persönlicher Bereicherung, sondern mehr nach Anerkennung, Geltung und Bewunderung.

▸ Aus materieller Not, zynischem Gewinnstreben oder sozialer Entwurzelung sind die kriminellen Hacker entstanden. Sie agieren in der Underground Economy, liefern Malware und das technische Knowhow für Botnetze, veranstalten DDoS-Angriffe oder drohen damit, um Geld zu erpressen, und dringen in fremde IT-Systeme ein, um Informationen zu stehlen, die sich zu Geld machen lassen. Für sie gilt die Aussage von Balduan aus dem Jahr 2008: Keiner hackt mehr heute zum Spaß, das ist knallhartes Business geworden [59].

▸ Nicht minder begabt und häufig nicht weniger skrupellos sind die IT-Söldner, die die Hacking-Methoden zum gewerblichen Einsatz verfeinern und einsetzen, sich dazu lautere Ziele auf die Fahnen schreiben und in der offenen Wirtschaft ihr Geld verdienen. Sie kommen erst nach und nach

Das Hacking war lange Jahre eine sportive akademische Besonderheit. Ihre spielerischen Protagonisten - die Hacker – waren von der Funktionsweise und den Möglichkeiten der IT begeistert, versuchten zu tricksen, fanden Sicherheitslücken und entwickelten bei diesen Gelegenheiten eine besondere Kultur, die zwischen zwei Extremen pendelt: Einerseits geht es ihr um die Absicherung der IT durch das Ausprobieren und Entdecken von Lücken und andererseits wurden mehr und mehr auch profitable Missbräuche praktiziert. Zunächst ging es dabei um zweierlei: Entweder um den parasitären Zugang zu sehr teurer Rechenzeit oder - mehr und mehr - um den Zugang zu geheimen Informationen anderer. Trotz aller Beteuerungen der "wir sind die Guten" bewegt sich das Hacking noch immer in diesem grauen Spannungsfeld.

1976 ist deshalb ein Meilenstein, weil erstmals die Hacking-Kultur einen Namen bekam und ihr spezifischer Sprachgebrauch dokumentiert wurde.

Dieter **Kochheim**, Eine kurze Geschichte der Cybercrime, 23.01.2011, S. 8

in das Gesichtsfeld der Öffentlichkeit [60]. HB Gary Federal, das französische Unternehmen Vupen [61] und die jüngsten Angriffsziele von LulzSec [62] liefern die Beispiele für die gewerblichen Söldner, die "gutes" Geld verdienen.

Weniger aus Spaß als aus Überzeugung handeln die Hacktivisten. Sie widmen sich dem Defacement, also dem Verschandeln gegenerischer Webseiten, führen DDoS-Angriffe durch und stehlen Daten. Auch sie unterscheiden sich nach ihren Motiven und Zielen.

▸ Noch wenig in Erscheinung getreten sind IT-Terroristen. Sie verfolgen politische Ziele und sind häufig von politischen oder religiösen Heilsvorstellungen geprägt, skrupellos und unbarmherzig.

▸ Viele Ähnlichkeiten mit den IT-Söldnern und -Terroristen dürften die regimetreuen Handlanger aufweisen. Sie übernehmen Auftragsarbeiten, bei denen die politischen Hinterleute im Dunkeln bleiben, und erlangen Anerkennung und wahrscheinlich auch Einkommen. Sie lassen sich im Zusam-

---

[56] Dieter **Kochheim**, Cybercrime und politisch motiviertes Hacking. Über ein Whitepaper von François Paget von den McAfee Labs, 20.10.2010

[57] Dieter **Kochheim**, Eskalationen, 20.02.2011, S. 24.

[58] Dieter **Kochheim**, Cybercrime – Cyberwar, 02.07.2011

[59] Gordon Bolduan, Digitaler Untergrund, Technology Review 4/2008, S. 26 ff.

[60] **CF**, IT-Söldner im Kampfeinsatz, 15.02.2011

[61] **CF**, Luigi, das kostet Dich etwas! 14.02.2011

[62] LulzSec hackt FBI-Liaison und Sicherheitsunternehmen, Heise online 04.06.2011

menhang mit DDoS-Angriffen in den GUS-Staaten und im Zusammenhang mit Spionageangriffen aus China erwarten.

Anonymous und LulzSec stehen eher in der Tradition der Spaß-Guerilla. Sie scheinen keinen politischen Programmen, aber individuellen, mehr moralischen Politikvorstellungen von Gut und Böse zu folgen. Auch wenn ihre Programmatik spontaneistisch und unprofessionell wirken mag, so sind das ihre Handlungen keineswegs [63], wie die Angriffe gegen Sony und HB Gary Federal anschaulich bewiesen haben.

Das intellektuelle und handwerkliche Hacking einerseits und der Einsatz von Malware andererseits ergänzen sich vielfach, wobei die Malware immer selbständiger und „automatischer" zu werden scheint.

Mit der Malware [64] wird ein Programm in das Zielsystem geschleust, dessen Sicherheitsvorrichtungen es unterläuft und abschaltet und sich schließlich einnistet und tarnt. Die weitere Penetration hängt von der Gestalt des Programms und den Motiven des Entwicklers ab. Die wichtigsten Gestaltungen betreffen den Betrieb eines Botnetzes [65], das Phishing [66] und neuerdings die Industriespionage (Night Dragon [67]).

Neben den Penetrationsstrategien sind im Zusammenhang mit der IuK-Kriminalität weitere Erscheinungsformen zu beobachten. Sie reichen von verteilten Angriffen (DDoS) über Schutzrechteverletzungen, Verbreitung verbotener Inhalte und von ideologischen Entgleisungen bis hin zur (weitgehend straflosen) Datenhehlerei und zu schlichten Betrügereien. Einzelne davon werden noch angesprochen. Zunächst geht es jedoch nur um die Frage, wie eine Penetration abläuft und wie sie als solche strafrechtlich begriffen werden kann.

Schadcode wird von Kriminellen über mehrere Wege verbreitet: Eine Möglichkeit ist das Hinterlegen von schädlichen Programmen auf Internetseiten. Schon der reine Besuch einer verseuchten Webseite reicht dabei aus, um den Computer über sogenannte Drive-by-Downloads mit Viren, Trojanern, Spionageprogrammen und weiterer Malware zu infizieren. Auf diese tückischen Internetseiten trifft der Nutzer entweder beim Surfen im Netz oder die URLs werden von den Tätern z. B. in sozialen Netzwerken oder durch Nachrichten in Chat-Programmen publiziert. Online-Kriminelle nutzen auch weiterhin Spam-Mails, um Anwender mittels Links auf präparierte Webseiten zu locken oder sie zu animieren, verseuchte Dateianhänge zu öffnen. Im Mail-Anschreiben ist dann beispielsweise die Rede von einer vermeintlichen Rechnung oder Mahnung oder es werden exklusive Fotos zu einem aktuellen Ereignis versprochen. Kommen die Anwender der Aufforderung nach, gelangen sie direkt auf die Schadcode-Seiten und fangen sich unbeabsichtigt einen Computerschädling ein.

G Data Security Studie 2011. Wie schätzen Nutzer die Gefahren im Internet ein? 20.06.2011

---

[63] Beides spiegelt sich in dieser Meldung wider: US-Sender wegen WikiLeaks-Bericht gehackt, Heise online 31.05.2011.

[64] **CF**, Malware, 12.05.2008

[65] **CF**, Botnetze, 2007

[66] **CF**, Phishing mit Homebanking-Malware, 22.10.2008

[67] **CF**, Night Dragon, 13.02.2011

2.3.1 Malware, Datenträger und Anhänge

Ein informationstechnisches System kann grundsätzlich nur über eine Schnittstelle penetriert werden [68]. Dazu kommen alle Formen von Wechseldatenträgern (Disketten, USB-Sticks, Wechselfestplatten, Speichersticks aus Kameras und Handys und selbst Magnetkarten [69]) in Betracht, vor allem aber die Verbindungen zum Internet selbst, das Funknetz (WLAN) und sogar ein separater Telefonnetzanschluss, wenn er über die Telefonanlage mit der Datenverarbeitung verbunden ist. Schließlich bieten auch alle Formen der Nahfunkverbindungen (Infrarot, Bluetooth und andere) und der Kabelanschluss einen denkbaren Einstieg, sogar das Stromnetz, wenn mit ihm eine Datenverbindung geliefert wird.

Die Transportmittel sind Dateien und Programme, die hier als Malware bezeichnet werden [70]. Sie sind als fremde Software zu definieren, die die Systemintegrität angreift, um eine bösartige Aktion auszuführen. Die Bösartigkeit kann zerstörerisch sein (Dateien löschen, System unbrauchbar machen), ausforschend (Keylogger, Suche nach persönlichen Daten und Geheimnissen) oder missbräuchlich (▸ modernes Phishing, ▸ Einbindung in ein Botnetz). Von ihrer Form her werden unterschieden:

Angriffsebene

- **Systemstart** (BIOS, EPROM)
- **Booten** (Betriebssystem, Kernel)
- **Programmumgebung** (Betriebssystem)
- **Anwenderoberfläche** (Windows, Linux)
- **Anwenderprogramme** (Office, Adobe, Browser)
- **laufender Betrieb** (Java, active X)

▷ Viren sind die älteste Form. Sie binden sich in eine bestehende Datei ein und bewirken ihre schädliche Funktion dadurch, dass sie zusammen mit ihr ausgeführt werden. Schon diese einfachsten Formen der Malware wurden mit intelligenten Eigenschaften versehen. Sie konnten sich in den Startvorgang einbinden (Bootviren) und sich tarnen (Stealthviren), indem sie den Zeitstempel der angegriffenen Datei und vor allem ihre Größe erhalten haben [71].

▷ Würmer sind selbständige Dateien, die einen laufenden Arbeitsprozess dazu ausnutzen, ihrerseits ausgeführt zu werden.

▷ Trojaner verstecken sich hinter einem nützlichen Dienstprogramm, das oberflächlich ausgeführt wird, und entfalten im Hintergrund ihre bösartigen Aktivitäten.

▷ Kommandostrings sind kurze Kommandofolgen, die in eine Webseite, eine andere Datei eingebunden oder an einen Link angefügt werden. Sie veranlassen einen Internet-Browser oder ein anderes Anwenderprogramm dazu, die Malware aus dem Internet zu laden.

Für die rechtliche Auseinandersetzung sind solche Definitionen fast ohne Bedeutung. Moderne Malware nutzt alle Erscheinungsformen, wechselt zwischen ihnen und ändert ihre Gestalt. Darauf kommt es rechtlich nicht an, weil nach ihrem Vorgehen und ihren Wirkungen zu fragen ist.

Das IT-Strafrecht orientiert sich an diesen Auswirkungen. So wendet sich § 202a Abs. 1 StGB gegen das Ausspähen von Daten. Trotz der formel-

---

[68] Alle – auch fernliegenden – Schnittstellen, die ich 2007 angesprochen habe, sind inzwischen zumindest als Übertragungsweg ausprobiert worden. Siehe: **CF**, IT-Sicherheit, Schwachstellen, Angriffe, 2007.
Stuxnet wendet sich destruktiv gegen Industrieanlagensteuerungen und wurde nur über USB-Sticks in die angegriffenen Systeme eingebracht. Die gegenwärtige Entwicklung, vor allem individualisierte Angriffe zum Zweck der Informationsspionage durchzuführen, macht auch „schwierige“ Schnittstellen wie den Nahfunk attraktiv, weil dazu sowieso alle Einzelschritte genau geplant und an die Gegebenheiten des einzelnen Zielsystems angepasst werden müssen. Dass die Tendenz genau in diese Richtung geht, hat der Night Dragon-Angriff gezeigt.

[69] Das ist bislang nur eine theoretische Überlegung. Der Magnetstreifen einer Identifikationskarte verfügt aber über genügend Kapazität, um einen Starterstring zu beherbergen.

[70] Der Code für die schädlichen Funktionen wird auch als Payload bezeichnet.

[71] Einzelheiten bei G Data, Malware-Geschichte (drei Teile).

len Datendefinition in § 202a Abs. 2 StGB darf nicht unbeachtet bleiben, dass die Vorschrift in dem Abschnitt über die „Verletzung des persönlichen Lebens- und Geheimbereichs“ angesiedelt ist und keine Strafbarkeit des Versuchs kennt. Deshalb kommt es nicht nur darauf an, dass der Angreifer überhaupt Daten, *die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind*, erlangt, sondern auch darauf, dass sie grundsätzlich einen gewissen Geheimniswert haben und nicht öffentlich präsentiert werden (▸ Ausspähen von Daten).

Dieser strafrechtliche Datenschutz wird noch verstärkt von § 274 Abs. 1 Nr. 1, 2 StGB, wonach die Vernichtung fremder technischer Aufzeichnungen und beweiserheblicher Daten mit Strafe bedroht ist.

§ 303a StGB über die Datenveränderung ist hingegen im Sachbeschädigungsrecht angesiedelt. Das führt dazu, dass nicht jede Datenveränderung strafbar ist, sondern nur die, die zu messbaren Daten- und Funktionsverlusten führt. Die Computersabotage (§ 303b StGB) lässt jedoch bereits die Zuleitung von Malware als Tathandlung genügen (▸ Datenveränderung. Computersabotage).

Die Fälschung beweiserheblicher Daten (§ 269 StGB) ist ein Teil des Urkundenfälschungsrechts. Das wiederum hat zur Folge, dass die Beweisbedeutung der Daten ausschlaggebend ist. Das setzt voraus, dass sie mit einer Person als Aussteller (der Urkunde) in Verbindung stehen müssen, der mit ihnen eine Aussage treffen will, die zumindest mittelbar eine Rechtsfolge betrifft. Daran ändert auch § 268 StGB über die Fälschung technischer Aufzeichnungen nichts. Beide Vorschriften schützen nur verschiedene – menschliche oder automatische – Verarbeitungsprozesse und verlangen gleichermaßen, dass die Daten Bedeutung für Rechtsfolgen haben müssen.

Schließlich wendet sich der Computerbetrug (§ 263a StGB) nicht gegen jede missbräuchliche oder täuschende Datenverwendung, sondern nur gegen die, die das Vermögen des berechtigten Dateninhabers beeinträchtigen kann.

Angriffsprozess:

Über eine ▸ ***Außenverbindung*** muss schädlicher Code in den Hauptspeicher des Zielsystems eingebracht (▸ ***Injektion***) und dort so verarbeitet werden, dass seine Funktionen ausgeführt werden (▸ ***Infektion***). Dazu wird eine Sicherheitslücke missbraucht (▸ ***Exploit***), die die Malware dazu nutzt, sich zu ▸ ***installieren***. Dazu erkundet sie in aller Regel die Umgebungseigenschaften und lädt von einem ▸ ***Command and Control-Server*** im Internet Updates und weitere Programmbestandteile. Anschließend versucht sie sich zu tarnen. Dazu kommen ▸ ***Rootkits*** zum Einsatz, also Programmpakete, die vorhandene Sicherheitseinrichtungen abschalten oder unterlaufen, mit denen die Malware zum jeweiligen Neustart eingebunden (▸ ***Einnisten***) und vor Entdeckung getarnt wird. So präpariert kann die Malware ihre schädlichen Funktionen ausführen, kann das System nach wertvollen Informationen durchsuchen (Lizenzschlüssel, Kontodaten, Zugangscodes), Arbeitsprozesse überwachen (Keylogger) und andere Aktionen steuern (Phishing, Botnetze, DDoS, Spams). Ganz häufig wird dabei auch eine Hintertür eingerichtet (▸ ***Backdoor***), die der Angreifer direkt dazu nutzen kann, das angegriffene System als Konsole für geheime Aktivitäten zu nutzen.

Ausschlaggebend sind also die tatsächlichen und rechtlichen Folgen, die mit dem Einsatz von Malware verbunden sind. Dazu reicht die Tatsache, dass schädlicher Code angeliefert wird, nur ausnahmsweise aus. Er muss auch gelesen werden, um zunächst in den Arbeitsspeicher des Zielgerätes zu gelangen (Injektion). Dazu bedarf es Tricks und vor allem einer Ablaufumgebung, in die sich der schädliche Code einbinden und seine eigenen Funktionen ausführen lassen kann (Infektion). Solche Ablaufumgebungen stellen handelsübliche Computer in reicher Anzahl.

Beim Start des Computers wird zuerst das BIOS ausgeführt [72]. Es lädt die Treiber für die angeschlossene Hardware (Tastatur, Maus, Hauptspeicher [Arbeitsspeicher] und Massenspeicher [Festplatte usw.]) und startet das Betriebssystem. Seine Anweisungen und Einstellungen bekommt das BIOS in aller Regel von einem Speicherchip, der Daten auch ohne Stromversorgung speichern kann (zum Beispiel EPROM [73]). Die Chips sind

[72] basic input/output system - BIOS

[73] Erasable Programmable Read-Only Memory - EPROM

speicherfähig und bieten damit die erste Gelegenheit, fremden Code in einen Verarbeitungsvorgang einzubringen [74].

Zur Infektion muss mehr geschehen, als den Code nur in den Arbeitsspeicher einzubringen. Der Computer muss auch einen Anlass haben, ihn zu verarbeiten.

Tatort Internet bei heise.de:

Thorsten **Holz**, Alarm beim Pizzadienst, c't 13/2010, S. 184 (Website Injection)

Frank **Boldewin**, Zeig mir das Bild vom Tod, c't 14/2010, S. 186 (Powerpoint)

Thorsten **Holz**, PDF mit Zeitbombe, c't 15/2010, S. 164 (PDF)

Sergei **Shevchenko**, Angriff der Killervideos, c't 16/2010, S. 178 (Shockwave-Flash)

Sergei **Shevchenko**, Matrjoschka in Flash, c't 17/2010, S. 170 (Shockwave-Flash)

Jasper **Bongertz**, Nach uns die SYN-Flut, c't 15/2011, S. 176 (DDoS)

Eduard **Blenkers**, Ferngesteuert, c't 16/2011, S. 174 (Zombie durch Fernwartung)

Frank **Boldewin**, Eine Reise ins RAM, c't 17/2011, S. 144 (Online Banking-Trojaner)

Frank **Boldewin**, Operation am offenen Herzen, c't 18/2011, S. 178 (Rootkit)

Die erste richtige Gelegenheit dazu bietet sich beim Booten des Betriebssystems. Es wird, gesteuert vom BIOS, von einem Massenspeicher geladen (interne Festplatte, externe Medien wie CD, DVD, USB-Stick) und richtet die Grundfunktionen des Computers ein. Das geschieht in der Regel zweistufig. Für die Feinsteuerung der Hardware ist der Betriebssystemkern (Kernel) verantwortlich und im zweiten Schritt werden die grundlegenden Programmroutinen installiert. Anschließend erfolgt in aller Regel die Einrichtung der Anwenderoberfläche, das heißt die Einrichtung der grafischen Bildschirmoberfläche, womit die wichtigsten Grundfunktionen des Computer zusammen geführt werden. Zeitgleich oder danach werden auch die Anwenderprogramme eingerichtet, die das Arbeiten (oder den Spaß) am Computer erst ermöglichen (Office, Browser für das Internet, Spiele).

Um aber überhaupt in den Verarbeitungsprozess zu gelangen, muss die Malware eine Sicherheitslücke ausnutzen (Exploit), also einen nicht oder nur schwach überwachten Arbeitsprozess im Computer. Am wenigsten geschützt ist der erste Startvorgang und es hat tatsächlich schon Viren gegeben, die das BIOS überschrieben und zerstörerische Wirkungen entfaltet haben (Festplatte formatieren). Die Möglichkeiten für die Installation und Inbetriebnahme ausgefeilter Malware sind jedoch auf dieser Ebene begrenzt. Moderne Betriebssysteme und Antivirusprogramme überwachen bereits den Bootvorgang im Hinblick auf Unregelmäßigkeiten, ungewöhnliche Ablaufprozesse (Heuristik [75]) und den Start unbekannter Programme. Das ist auch nötig, weil sich besonders ausgefeilte Malware in den Bootvorgang einzubringen versucht, indem Treiberdateien verändert, ausgewechselt oder hinzugefügt werden.

Bevor es dazu kommt, muss die Malware zunächst Ablaufprozesse infizieren und sich als Programm installieren. Am häufigsten werden dazu Exploits auf der Ebene der Anwenderprogramme missbraucht. Dazu werden ganz häufig die Anhänge zu E-Mails genutzt. Sie sind funktionstüchtige Dateien, die mit ihrem Suffix [76] die Anwendungsumgebung anfordern, die sie ausführen kann. Diese Umgebungen lassen vielfach umfangreiche und tiefe Programmabläufe zu, so dass sie dazu missbraucht werden können, ein fremdes Programm zu installieren. Gegenwärtig fußen die meisten Missbräuche auf dem Acrobat Reader von Adobe und auf der Laufzeitumgebung Java von Oracle (vormals Sun) [77]. Die Browserhersteller (MS Outlook, Thunderbird u.a.) haben darauf reagiert und lassen in aller Regel keinen automatischen Start von E-Mail-Anhängen zu.

---

[74] Das gilt auch für alle Schnittstellen, zum Beispiel für die Grafik-, Sound- oder TV-Karte, die auf Systemebene betriebsbereit gemacht werden.

[75] Antivirenprogramm. Heuristik

[76] Suffix ist die Zeichenfolge, die dem Dateinamen nach einem Punkt rechts angefügt ist. „doc“ steht zum Beispiel für Microsoft Office Word, „pdf“ für den Acrobat Reader von Adobe und „htm“ (html) für eine browserfähige Datei in der Skriptsprache Hypertext Markup Language.

[77] Kaspersky-Studie: Adobe-Software größtes Sicherheitsrisiko, Heise online 16.08.2011

Ein wichtiges Einfallstor liefern die Browser für die Anzeige von Internetseiten (Internet Explorer, Firefox u.a.). Diese beruhen ganz überwiegend auf der einfachen Skriptsprache Hypertext Markup Language – HTML, die nur wenige Möglichkeiten zum Missbrauch bietet. Eine beliebte davon sind die „iFrames“.

Frames bieten die Möglichkeit, verschiedene Seiten zur gemeinsamen Ansicht zu kombinieren, zum Beispiel dazu, um einen Bereich des Bildschirms fest zur Navigation zu bestimmen und einen anderen als Textcontainer, der „gescrollt“ werden kann. Dazu wird zunächst eine Datei geladen, die Fenster definiert und die ausfüllenden Dateien lädt. Dasselbe geschieht mit eingebetteten Frames, also mit iFrames. Sie definieren auf einer Seite ein Fenster, in dem eine andere Datei angezeigt wird und laden diese gleichzeitig [78]. Die Größe der Anzeige lässt sich einstellen und die Breite und Höhe können auch auf Null gestellt werden. Dann lädt der Browser eine Datei, die nicht angezeigt wird, und es kann sich um Malware handeln, die zunächst den Browser und damit auch den Hauptspeicher mit schädlichem Code injiziert.

Daneben lässt HTML auch die Einbindung von Skript-Kommandos und von Multimedia-Elementen zu (Bilder, Sounds, Videos, Flash-Animationen), die ihrerseits mit Malware infiziert sein können. Das meiste davon fangen die aktuellen Browser und Antivirenprogramme ab, wenn sie auf aktuellem Stand und die betreffenden Exploits eingestellt sind [79].

Malware – egal zu welchem Zweck – nistet sich in aller Regel durch Exploits im laufenden Betrieb (Internetbrowser, Java), durch verbreitete Anwenderprogramme (z.B. Acrobat Reader) oder in allen Verarbeitungsstufen über Wechseldatenträger ein. Meistens werden dazu die nötigen Programmteile und Updates aus dem Internet geladen und im angegriffenen System installiert. In diesen Fällen kann der schädliche Code in einem relativ kurzen Kommandostring bestehen, der das Anwenderprogramm zum Laden des noch im Internet vorgehaltenen Programms anweist. Erst dann nistet sich die Malware dauerhaft im System ein und das bevorzugt auf der Ebene des Betriebssystems und seltener (aber effektiver) auf der Ebene des Kernels. Dazu trägt es sich zum Beispiel in die Auto-Start-Bereiche der Registry unter Windows, in andere AutoStart-Dateien oder in Laufzeit-Bibliotheken ein, die beim Booten oder dem Start von üblichen Anwenderprogrammen ausgeführt werden. Seine Programmbestandteile versteckt sie mit Hilfe von Rootkits in den System- oder anderen Dateien, von denen erwartet wird, dass sie selten oder nie durchleuchtet werden. Kernfunktionen der Malware, die sich den Virenscannern durch ihre Funktionalität verraten könnten, werden dazu häufig verschlüsselt, solange sie nicht ausgeführt werden.

---

[78] Das Gästebuch des Cyberfahnders ist ein praktisches Beispiel für einen iFrame.

[79] Bislang ganz unbekannte Schwachstellen werden auch Zero-Day-Exploits genannt. Das bedeutet, dass sie zuvor Null Tage bekannt waren, bevor sie von einer Malware missbraucht werden. Die mangelnde Aussagekraft dieses Begriffes wird von Muttik von McAfee zu recht kritisiert: **CF**, Zero-Day-Exploits und die heile Hackerwelt, 06.11.2010. Auch solche Exploits können anhand ihrer Abläufe und Wirkung erkannt werden (Heuristik).

2.3.2 fortgeschrittene Techniken

Die Beiträge in diesem Kapitel widmen sich aktuellen Erscheinungsformen beim Einsatz von Malware. Dabei geht es darum, die hohen Entwicklungsstände der Malware-Technik und die detaillierten und professionellen Ablaufplanungen der Angreifer zu veranschaulichen.

Die ersten beiden Erscheinungsformen sind allgemeiner Art und offenbaren besonders die Rücksichtslosigkeit, mit der IuK-Kriminelle Malware zu ihren Zwecken einsetzen.

Das Thema ▸ Phishing beschränkt sich hier auf ein Beispiel des Identitätsdiebstahls beim Onlinebanking und könnte zu vielen Varianten ausdifferenziert werden. Es hebt sich von vielen anderen Beispielen dadurch hervor, dass die kriminelle Aktion nur im Zusammenspiel zwischen einer hochentwickelten Malware auf dem Computer des Betroffenen und einem Command and Control-Server – C&C – abgewickelt wird, ohne dass es seitens des Angreifers noch eines menschlichen Zutuns bedarf. Bei dem Text handelt sich um eine Zusammenfassung vieler Meldungen in Onlinediensten, der Tagespresse und polizeilichen Erfahrungen.

Beim Identitätsdiebstahl geht es immer darum, persönliche (Echt-) Daten mit dem Ziel auszuspähen, mit ihnen Zugang zu fremden Online-Konten zu bekommen, um mit den fremden Daten Leistungen zu erlangen, Geschäfte abzuschließen, die zulasten des Kontoinhabers gebucht werden, oder um sich unter fremder Identität im Internet und anderswo zu bewegen [80]. Online-Konten in diesem Sinne sind nicht nur Bankkonten, sondern alle Accounts, die Zugang zu exklusiven Diensten und Leistungen gewähren. Sie können bei Handelsplattformen wie Amazon oder eBay bestehen, bei Warenhäusern, Informationsdiensten (Fachinformationen, Zeitungen, Wetterdienst), virtuellen Veranstaltungen wie Second Life oder geschlossenen Spielen, zu Versanddiensten wie DHL, UPS und Packstationen sowie schließlich zum Onlinebanking und anderen Bezahldiensten wie PayPal, E-Gold und WebMoney. Angegriffen und missbraucht werden alle Dienste, mit denen werthaltige Leistungen ertrogen oder erschlichen werden können.

Die Funktionsweise von ▸ Botnetzen ist schon an anderer Stelle breit beschrieben worden [81], so dass hier nur eine Zusammenfassung und Würdigung erfolgt.

Die vier weiteren Beispiele widmen sich aktuellen Malware-Projekten, die 2010 und 2011 öffentlich bekannt geworden sind. Sie sind hochgradig professionell und richten sich immer ganz gezielt gegen ausgesuchte Unternehmen und Organisationen, wobei nicht nur besonderes Wissen über die Konstruktion von Malware als solche nötig ist, sondern auch über den internen Technikeinsatz, die innere IT-Struktur und die Unternehmensorganisation.

Eine hervorgehobene Rolle spielt dabei ▸ Stuxnet. Diese Malware ist wahrscheinlich mit einem beispiellosen finanziellen Aufwand speziell dazu entwickelt worden, die Atomanreicherungsanlagen im Iran zu sabotieren. Sie hebt sich von kriminellen Angriffen dadurch ab, dass sie sich über Speichermedien verbreitet, mehrere hochwertige Exploits und Rootkits zur Infektion, Einnistung und Ausführung einsetzt und schließlich ganz langfristig und gezielt Industrieanlagensteuerungen der Firma Siemens sabotiert. Der Angriff gegen solche Steuerungen ist bislang beispiellos.

Die übrigen drei Projekte betreffen groß angelegte Formen der Industriespionage, die jeweils Besonderheiten aufweisen. ▸ Shady RAT ist erst im Frühjahr 2011 nach fünf Jahren Laufzeit öffentlich bekannt geworden. Es richtet sich gegen weltweit 72 Unternehmen und Organisationen und hebt sich auch dadurch hervor, dass eine unvorstellbare Datenmenge gestohlen wurde (vermutlich in Petabyte-Größe).

▸ Aurora richtete sich Ende 2009, Anfang 2010 gegen Google und 30 weitere Unternehmen, die be-

---

[80] Dieter **Kochheim**, Cybercrime, 24.05.2010, S. 45, m.w.N.

[81] Dieter **Kochheim**, Cybercrime, 24.05.2010, S. 55

vorzugt in China engagiert waren. Die Ausführung kann als klassisches Beispiel für einen Malware-Angriff gesehen werden, mit dem sich der Angreifer eine Hintertür (Backdoor) zu Firmennetzen verschafft haben, um dann Unternehmensgeheimnisse zu stehlen. Wegen seiner Anschaulichkeit wird anschließend anhand des ▸ Aurora-Beispiels das IuK-Strafrechts im engeren Sinne praktisch angewendet.

Den fortschrittlichsten Angriff zeigte der ▸ Night Dragon. Er hebt sich dadurch hervor, dass die Angreifer nicht nur zielgenau in die Firmennetze von petrochemischen Unternehmen eingedrungen, sondern aus dem Innern der Unternehmen heraus über gesicherte VPN-Tunnel direkt auf die Laptops leitender Firmenangehöriger gelangt sind.

2.3.2.1 Phishing

Die Zeiten, in denen unbedarfte Homebanking-Kunden mit E-Mails dazu aufgefordert wurden, ihre Zugangsdaten und TAN zu offenbaren [82], sind längst vorbei. Die dazu verwendeten Überredungstechniken (Social Engineering [83]) kommen heute immer noch in anderen Zusammenhängen zum Einsatz [84]. Modernes Phishing funktioniert hingegen als Man-in-the-Middle-Angriff [85], bei dem die Malware die zentrale Rolle spielt.

Die eingenistete Malware wartet darauf, dass der Anwender eine der bekannten Homebanking-Webseiten aufruft. Seine Zugangsdaten fängt sie ab und protokolliert sie, bis der komplette Anmeldevorgang abgeschlossen ist. Das ist nötig weil die heute üblichen Captchas [86], kleine Bilder, die Ziffern und Zeichen nur verzerrt wiedergeben, den automatischen Zugang erschweren. Die direkte Verbindung zwischen Anwender und Bank wird dann von der Malware gekappt und sie klemmt sich quasi als Router zwischen alle weiteren Vorgänge. Ganz viele individuelle Daten – Name, Kontonummer, Kontostand und letzter Besuch – offenbaren die Homebanking-Portale von sich aus. Sie gibt die Malware an einen Command and Control-Server – C&C – weiter, der ihr dann eine gefälschte Begrüßungsseite übermittelt, die die Malware auf den Bildschirm ausgibt. Dabei gaukelt sie zum Beispiel eine sichere „shttp“-Verbindung mit dem Server der Bank vor.

Das weitere Vorgehen variiert. Gelegentlich generiert der C&C jetzt einen Sicherheitshinweis: Wir haben das Homebanking grandios sicher gemacht. Um die neuen Sicherheitsfunktionen nutzen zu können, geben Sie bitte die iTAN Nummer

---

82 So noch: **CF**, Phishing, 2007

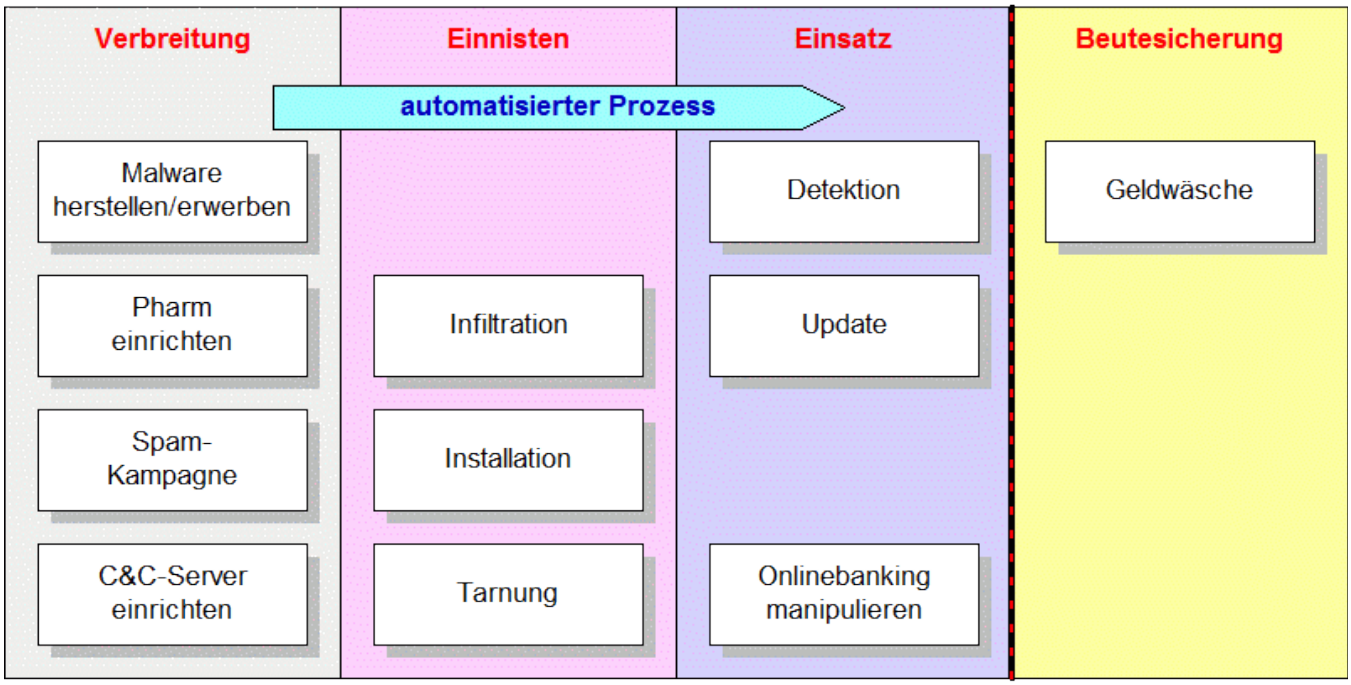
83 **CF**, Fünf unwichtige Informationen ergeben eine sensible, 01.03.2009

84 Sabrina **Berkenkopf**, Ralf **Benzmüller**, Gefährliche E-Mails, G Data Whitepaper 6/2011, 01.06.2011

85 Am häufigsten sind jetzt die Fälle des Man-in-the-Browser, wobei sich die Malware in der Umgebung des Internet-Browsers festsetzt und als Schaltstelle das Onlinebanking überwacht und manipuliert.

86 CAPTCHA

Tatphasen beim Einsatz von Onlinebanking-Trojanern



Schematische Darstellung der Tatphasen beim Einsatz von autonomen Onlinebanking-Trojanern. Die Täter müssen vor allem in der ersten Phase der Vorbereitung aktiv handeln, um die Malware zu entwickeln oder zu beschaffen und ihre Verbreitung vorzubereiten. Anschließend startet ein automatisierter Prozess, der kein oder nur sehr wenig menschliches Eingreifen bedarf.

Die Infiltration, Installation und Tarnung der Malware erfolgt selbständig im Zusammenwirken von Trojaner und C&C Server.

Verschiedene Varianten erkunden den Datenbestand des eroberten Zombies und melden Zugangs- und andere „interessante“ Daten an den C&C (Detektion). Im übrigen wartet die Malware darauf, dass der Anwender mit dem Homebanking beginnt, um dann erbarmungslos aktiv zu werden.

Die rechtlichen Bewertungen wegen der einzelnen Tatphasen erfolgen unter ▸ Onlinebanking.

soundso ein! Derweil hat die Malware mit vom C&C angelieferten Daten eine Überweisung an Igor Popow vorbereitet. Die abgefragte iTAN ist genau die, die zur Bestätigung der Überweisung gebraucht wird. Die Rückmeldungen der Bank werden von der Malware unterdrückt und die Startseite der Bank mit Hilfe des C&C so präsentiert, als wäre die Überweisung nie geschehen.

Der Anwender gibt seine eigenen Überweisungsdaten ein und das böse Spiel wiederholt sich. Die Malware fängt die eingegebenen Daten ab und generiert im Zusammenspiel mit dem C&C eine Transaktion an Vladimir Vostok. Die Bank fordert eine neue iTAN und der C&C verwendet die vom Anwender eingegebenen Daten, um eine neue Seite zu erstellen, die die Rückmeldung der Bank vorgaukelt und zur Eingabe eben dieser iTAN auffordert. Damit bestätigt die Malware die Überweisung an Vostok und der C&C wandelt die Rückmeldung so um, als wäre des Anwenders Anweisung ausgeführt worden. Das lässt sich beliebig wiederholen. Sobald der Anwender das Homebanking-Portal verlässt, kappt die Malware die Internetverbindung und ändert die lokale DNS-Tabelle (die in die Registry eingebunden ist), so dass beim Besuch der eigenen Bank nur noch eine Fehlerseite aufgerufen oder der Internetzugang insgesamt verhindert wird.

Merken das die Banken nicht? Doch, sie setzen Prüfmechanismen ein und können ungewöhnliche Aktivitäten erkennen. Der C&C steht zwar womöglich in der Ukraine, aber zum Zugang zur Bank nutzt er einen Zombie aus einem Botnetz aus der räumlichen Nähe des Anwenders als Konsole.

Zahlungsempfänger ist auch nicht „Igor Popow“ in Odessa, sondern „Waltraut Meier“ in Oberhausen oder Zicherie. Sie leitet das Geld als Finanzagentin auf verschlungenen Wegen an Popow weiter. Ihr Konto wird später mit dem Überweisungsbetrag rückbelastet und sie wegen leichtfertiger Geldwäsche mit Geldstrafe bestraft (§ 261 Abs. 5 StGB). Finanzagenten sind Kanonenfutter und können nur wenige Male eingesetzt werden. Deshalb sind die Täter auch dazu übergegangen, (im Ergebnis erfolglos) Arbeit suchende Ausländer Bankkontos im Inland eröffnen zu lassen oder Konten unter falschen Identitäten zu errichten. Ausweispapiere, Post-Ident-Unterlagen und Gehaltsbescheinigungen lassen sich dank Photo-Shop leicht fälschen und einfach verwenden, wenn die Bank die Übermittlung als Fax-Kopie akzeptiert [87].

[87] Was regelmäßig eine Verurteilung wegen Urkundenfälschung (§ 267 StGB) – Gebrauch einer falschen Urkunde – ausschließt. Die Kopie oder das Abbild eines Fax', die keinen anderen Eindruck erwecken, als eben eine Kopie oder ein Faxausdruck zu sein, sind keine Urkunden mit dem Aussagegehalt des Originals: **BGH**, Beschluss vom 27.01.2010 - 5 StR 488/09.

2.3.2.2 Botnetze

Botnetze [88] sind die mächtigsten Werkzeuge [89], die der Cybercrime heute zur Verfügung stehen [90].

Ein Botnetz, auch Zombie-Netz genannt, ist ein Zusammenschluss von Computern, die mit einem Schadprogramm infiziert sind. Es ermöglicht Cyberkriminellen die Fernsteuerung der befallenen Rechner, ohne dass Anwender etwas davon bemerken. Zombie-Netze können inzwischen auch ohne größeres Fachwissen aufgebaut und gesteuert werden. Sie sind daher lukrativ einsetzbar. Die Folge: die Anzahl von Botnetzen wächst (Namestnikov [91]) mit steigender Tendenz [92].

Genaue Zahlen über die Anzahl von Botnetzen liegen mir nicht vor. Vermutlich sind etwa zwei Dutzend Banden weltweit führend, die sich anhand der eingesetzten Malware, ihrer digitalen Handschriften und Werbestrategien unterscheiden lassen. Durch die zunehmende Verbreitung von Baukästen für die Zusammensetzung von „Botware“ dürfte die Anzahl der kleinen Botnetze noch sprunghaft ansteigen, auf Dauer für die Hersteller von Antivirenprogramme aber kein ernsthaftes Problem darstellen.

Die mit Malware infizierten Zombies verhalten sich inzwischen sehr zurückhaltend und unauffällig, um den Anwender möglichst wenig zu beeinträchtigen [93]. Das ist der Ökonomie geschuldet. Ein Zombie

[88] **CF**, Botnetze, 2007

[89] **CF**, mächtige Werkzeuge für die Cybercrime, 24.09.2010;
Zheng **Bu**, Pedro **Bueno**, Rahul **Kashyap**, Adam **Wosotowsky**, Das neue Zeitalter der Botnets, McAfee 19.08.2010.

[90] Sturmwurm-Botnetz sperrangelweit offen, Heise online 09.01.2008;
CF, Basar für tatgeneigte Täter. Botnetze, 11.04.2010

[91] Yuri **Namestnikov**, Schattenwirtschaft Botnetz – ein Milliongeschäft für Cybercriminelle, Kaspersky 24.07.2009

[92] Schädlingsbaukästen befeuern Botnetzepidemie, Heise online 17.02.2011;
Damballa, Top 10 Botnet Threat Report – 2010, 11.02.2011

[93] Zum Verhalten von Botnetzen: Tom **Simonite**,

ist wertvoll und soll möglichst lange unentdeckt und missbrauchsfähig bleiben. Sein behutsamer Einsatz ist keine Freundlichkeit, sondern Kalkül. Hat er seine Schuldigkeit getan, wird er ohne Bedenken geopfert [94].

Mit Botnetzen lassen sich Spams und mit Malware verseuchte Nachrichten versenden. Die Zombies lassen sich ausforschen und zum Phishing missbrauchen. Außerdem dienen sie zu verteilten Angriffen (DDoS), lassen sich zur Erpressung nutzen, als verteilte C&C-Server (Flux-Server), als Speicherplattform für Drops (abgelegte, ausgespähte Daten) und andere illegale Inhalte, zum Download, zum verteilten Rechnen, um Zugangscodes oder Bitcoins zu knacken [95], und schließlich als Konsole zur verdeckten Kommunikation.

Die Programmierer von Botware müssen firm sein im Filesharing, der Fernwartung, im Missbrauch von Exploits (Schwachstellen in Programmen), im Einsatz von Rootkits (Tarnung) und den schädlichen Funktionen, die ausgeführt werden sollen. Dazu gehören auch Kenntnisse über wirtschaftliche Prozesse (Homebanking, Kursmanipulationen, Finanztransaktionen), das Social Engineering, um den Anwender zu übertölpeln und unachtsam zu belassen, und soziale Kompetenz, um sich vor der Strafverfolgung oder anderen peinlichen Nachstellungen zu schützen.

Eine solche Anforderungspalette können Einzelpersonen kaum leisten. Paget hat 2010 geschätzt, dass für den Betrieb eines Botnetzes zwei bis drei gute Programmierer nötig sind [96]. Hinzu dürften mindestens zwei Leute für die Logistik kommen, die die Werbung, den Einkauf, die Kundenbetreuung, den Zahlungsverkehr und die interne Qualitätskontrolle abwickeln. Balduan hat schon 2008 über Operating Groups berichtet, die aus mehreren Handwerkern und einem "Kopf" bestehen, der über Aufträge verhandelt, die Arbeit den Handwerkern zuteilt und überwacht und schließlich den Lohn verteilt [97]. Das gilt besonders auch für die Entwicklung von Malware, wobei Balduan Exploit-Händler und Rootkit-Entwickler als unabhängige Zulieferer ansieht.

2.3.2.3 Stuxnet

2010 wurde Stuxnet bekannt und die Firma Symantec hat sich besonders um seine Feinanalyse gekümmert [98]. Über diese besondere Malware lassen sich unter Vorbehalt einige Aussagen treffen:

Stuxnet ist eine Malware, die ganz gezielt zur Sabotage gegen die iranischen Atomanreicherungsanlagen in Natanz geplant und eingesetzt wurde. An ihrer Entwicklung waren seit 2007 mindestens zwei Entwicklerteams beteiligt, deren „Handschriften“ darauf schließen lassen, dass sie nicht der üblichen Malware-Szene entstammen, sondern dass sie eher Profis aus Israel oder den USA sind.

Seit dem Sommer 2009 wurden Mitarbeiter von Firmen, die an dem Bau der Atomanlage beteiligt sind, gezielt mit der Malware ausgestattet, die wahrscheinlich auf USB-Sticks gespeichert war und damit injiziert wurde.

Zur Infektion und Installation wurden mehrere Exploits verwendet, die bis zum Sommer 2010 unbekannt waren (Zero-Day-Exploits) und einen Schwarzmarktpreis im sechsstelligen Bereich erzielen konnten [99]. Auch die eingesetzten Rootkits waren bis zu ihrer Entdeckung unbekannt. Die

---

Botnetz unter der Lupe, Technology Review 21.12.2010;
CF, Zombies im Labortest, 21.12.2010.

94 Ausführlich zur Funktionsweise: Daniel **Plohmann**, Elmar **Gerhards-Padilla**, Felix **Leder**, Botnets: Detection, Measurement, Disinfection & Defence, ENISA 14.03.2011;
Jens **Tölle**, Botnetze: Erfassung, Messung, Desinfektion und Abwehr, Fraunhofer 2011

95 Trojaner nutzt GPU zur BitCoin-Gewinnung, Heise online 17.08.2011

96 Zum Spamming mit Botnetzen: François **Paget**, Cybercrime and Hacktivism, McAfee 15.03.2010, S. 44.

97 Gordon Bolduan, Digitaler Untergrund, Technology Review 4/2008, S. 26 ff.; kostenpflichtiger Download.

98 Nico **Ernst**, Stuxnet greift nur bestimmte Industrieanlagen an, golem.de 15.11.2010

99 Über € oder $ muss man sich wegen der nahen Wechselkurse keine Gedanken machen.

Entwicklungskosten werden im siebenstelligen Bereich vermutet.

Stuxnet ist in der Lage, ganz gezielt die Industrieanlagensteuerungen der Firma Siemens anzugreifen, die im Iran (dem Vernehmen nach nicht immer lizenzsicher) eingesetzt werden. Auch dazu bedarf es eines ganz besonderen Know Hows und Insiderwissens.

Stuxnet weist somit einige bislang nicht beobachtete Besonderheiten auf:

- die Malware ist extrem teuer in der Herstellung,
- richtet sich ganz gezielt gegen ein Angriffsziel,
- wird nicht über das Netz, sondern über Datenträger verbreitet,
- nutzt mehrere bislang unbekannte Schwachstellen (Exploits) und
- Rootkits und
- greift ganz gezielt Industrieanlagensteuerungen eines führenden Anbieters an.

Damit repräsentiert Stuxnet eine neue Qualität von Gefahr, die ich dem kalten Cyberwar zuordne [100]. Die Grafik oben stammt von McAfee [101] und ist deshalb besonders witzig, weil sie das bekannt gewordene Aufkommen der Malware visualisiert – geballt in Indien und Umgebung, nicht aber im Iran. Ein Schuft …

[100] Dieter **Kochheim**, Eskalationen. Stuxnet, 20.02.2011, S. 7, 8 m.w.N.

[101] Threat-Report: Drittes Quartal 2010, McAfee Labs 08.11.2010, S. 9.

2.3.2.4 Aurora

Seit Ende 2009 wurden Google und 30 weitere Unternehmen mit einer äußerst professionell programmierten Phishing-Malware angegriffen, die eine erst kurzfristig bekannt gewordene Sicherheitslücke im Internet Explorer ausnutzte [102]. Sie soll besonders darauf ausgerichtet gewesen sein, Zugangsrechte, Passwörter und Unternehmensgeheimnisse auszuspähen [103]. Der McAfee Threat Report für das erste Quartal 2010 [104] hebt die Rolle Chinas im Zusammenhang mit Sicherheitsbedrohungen hervor und sieht in der "Operation Aurora" <S. 12> *den bedeutendsten gezielten Angriff in der Geschichte des Internets*. Kurz zuvor hatte McAfee eine Studie herausgegeben, die sich mit dem Angriff im einzelnen auseinander setzte [105]. Sie zeigt genau die Arbeitsschritte, die oben (Malware, Datenträger und Anhänge) beschrieben werden, also zunächst die Anlieferung [106]:

1. *Ein ins Ziel geratener Benutzer bekam aus einer „vertrauenswürdiger“ Quelle einen Link in einer E-Mail oder in einer Sofortnachricht.*

2. *Der Benutzer klickte den Link an und gelangte so auf eine Webseite in Taiwan, die Schadcode in Form von schädlichem JavaScript-Payload enthielt.*

Darauf folgt die Injektion:

3. *Dieses schädliche JavaScript enthielt ein Zero-Day-Exploit für den Internet Explorer und wurde vom Browser des Benutzers heruntergeladen und ausgeführt.*

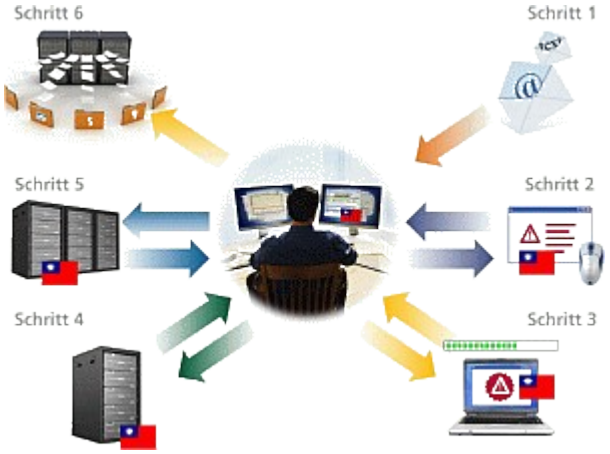
[102] Christoph H. **Hochstätter**, Aurora: Angriff mit IE-Exploit aus China auf Google und den Rest der Welt, zdnet 19.01.2010

[103] Marcel **Rosenbach**, Thomas **Schulz**, Wieland **Wagner**, Operation Aurora, Der Spiegel 18.01.2010

[104] McAfee Threat-Report: Erstes Quartal 2010, 12.05.2010

[105] Schutz für Ihre wichtigsten Ressourcen. Lehren aus „Operation Aurora“, McAfee Labs 12.04.2010

[106] Die Zusammenfassungen von McAfee sind bereits so komprimiert, dass sie durch eine Wiedergabe in eigenen Worten an Aussagewert verlieren würden. Sie werden deshalb im Wortlaut zitiert. Auch die Grafik stammt aus der Studie von McAfee.



Bis zu diesem Stadium ist noch nichts Schädliches geschehen. Schließlich folgt die Infektion:

4. *Der Exploit lud dann von Servern in Taiwan einen als Bild getarnten Binärcode herunter und führte den schädlichen Payload aus.*

Danach nistet sich die Malware ein:

5. *Der Payload richtete eine Backdoor ein und verband sich mit einem Botnet in Taiwan.*

Die Schaffung einer „Hintertür“ (Backdoor) ist eine der einfacheren Ausführungsfunktionen einer Malware, aber besonders geeignet zur Industriespionage, weil sie das unbemerkte Ausspähen von Daten im Unternehmensnetz ermöglicht:

6. *Damit hatten die Angreifer vollen Zugriff auf die internen Systeme. Sie hatten es auf geistiges Eigentum und Systeme zum Software-Konfigurations-Management (Software Configuration Management, SCM) abgesehen, auf die sie nun durch die gefährdeten Systeme Zugriff hatten. Das kompromittierte System ließ sich zudem so manipulieren, dass die Angreifer noch weiter in das Netzwerk vordringen konnten.*

Aurora ist ein Beispiel für einen eher klassischen Angriff, bei dem die Malware, anders als bei ▸ Stuxnet oder den ▸ Homebanking-Trojanern, keine dauerhaften, automatisch gesteuerten Aktivitäten ausführt, sondern dem Hacker nur den Zugang zum System verschafft. Das ändert nichts daran, dass hierzu besonderes Expertenwissen und Kenntnisse über das technische Innenleben der angegriffenen Unternehmen nötig waren. Diese Kombination aus präzisem Wissen, zielbewusstem Vorgehen und das gleichzeitig gegen eine ganze Reihe von Unternehmen zeichnet Aurora als eine neue Qualität bei den Angriffen im Internet aus.

2.3.2.5 Night Dragon

In einem nur in englischer Sprache verfügbaren White Paper berichtet McAfee über einen seit November 2009 offenbar von China aus geführten, koordinierten und gezielten Cyberangriff gegen globale Öl-, Energie- und petrochemische Unternehmen, dem McAfee den Namen Night Dragon gegeben hat [107]. Mit den Angriffen sollen vor allem Produktions- und Förderdaten, Informationen über Vorräte, Vertragsangebote und Projektkalkulationen erlangt werden.

Das Beispiel belegt, dass nicht nur die zerstörerischen DDoS-Angriffe gezielter werden, sondern auch die Hacking-Angriffe, die der Informationsbeschaffung und der Zerstörung dienen.

Bei dem Angriff geht es darum, den Fernzugriff auf die Computersysteme der angegriffenen Unternehmen mit entsprechenden Werkzeugen – Remote Access Tools - RAT - zu erlangen. Dazu werden Schwachstellen im Betriebssystem von Microsoft Windows und besonders in der Nutzerverwaltung und Rechtesteuerung - Active Directory - missbraucht.

Zunächst wird der Webserver des Unternehmens mit SQL-Injection-Methoden angegriffen. Dieser Webserver befindet sich noch außerhalb der engeren Schutzzone und dient den Kundenkontakten. Aber auch dazu muss er auf Kundendatenbanken, Preislisten und andere interne Informationen zugreifen. Das macht das Gesamtsystem anfällig.

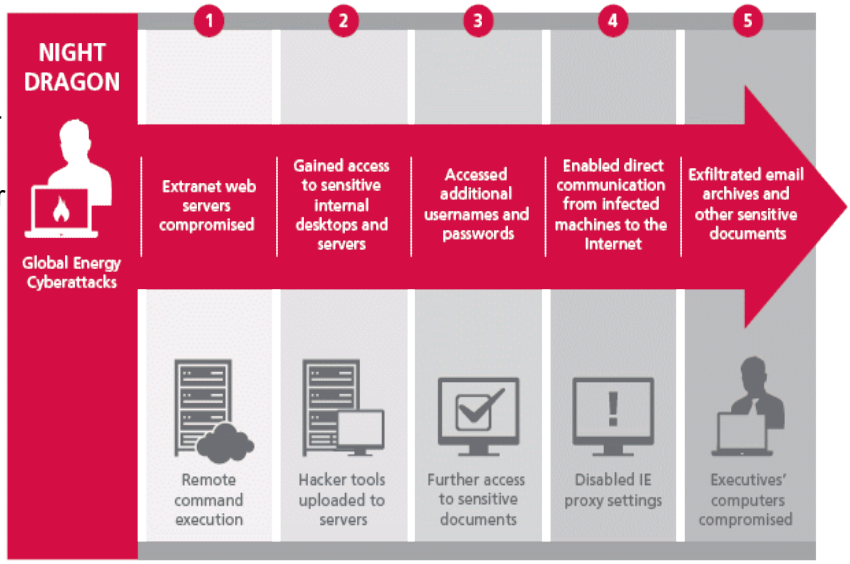
Die SQL-Injektion ist ein einfacher Kommando-String zur Steuerung von Datenbankfunktionen.

---

[107] Global Energy Cyberattacks: “Night Dragon”, McAfee Labs 10.02.2011;
Grafik Folgeseite: ebenda;
Stephen **Shankland**, Operation "Night Dragon": Hacker spionieren Ölindustrie aus, zdnet.de 10.02.2011

Gelingt es damit, die Kontrolle über den Webserver zu erlangen, können Hackerwerkzeuge nachgeladen (Infektion), Kontodaten und Zugangscodes ausgespäht oder protokolliert werden. Damit steht der Weg ins Innere des Unternehmensnetzes, alle Server und Desktoprechner offen.

Der Drache nutzt dazu verseuchte Webseiten, die der "eigene" Webserver den Mitarbeitern im Innern sendet, und E-Mail-Anhänge, die er auf dem firmeneigenen E-Mail-Server präpariert.



Um den Fernzugriff vom Command and Control-Server - C&C - des Angreifers durchzulassen, müssen nämlich die Sicherheitseinstellungen im Internet Explorer der firmeninternen Anwender und im Proxy-Server des Unternehmens abgeschaltet werden.

Der Night Dragon war offenbar erfolgreich. Über in China gehostete C&C-Server und Hostspeicher in den USA und den Niederlanden gelang der Eingriff gegen Unternehmen und gegen Führungskräfte in Kasachstan, Taiwan, Griechenland und den USA. Erlangt wurden neben sensiblen Unternehmensdaten auch urheberrechtlich geschützte und vertrauliche Informationen.
Mit neu entwickelten und angepassten Software-Werkzeugen schaffte es der Drache, Firewalls und VPN-Tunnel zu durchdringen, um auf die Laptops der sich sicher glaubenden Mitarbeiter und Führungskräfte zu gelangen.

Diese Angriffstiefe ist neuartig. Der Night Dragon gelangte nicht nur in die Firmennetze hinein, sondern schaffte es, die als sicher geltenden VPN-Verbindungen (nicht zu durchbrechen, sondern schlicht) zu umgehen, indem er sie von der Quelle im Unternehmenskern an nutzt. Jede noch so qualifizierte, aber aufgesetzte Sicherheitstechnik kann auf diese Weise ausgehebelt werden.

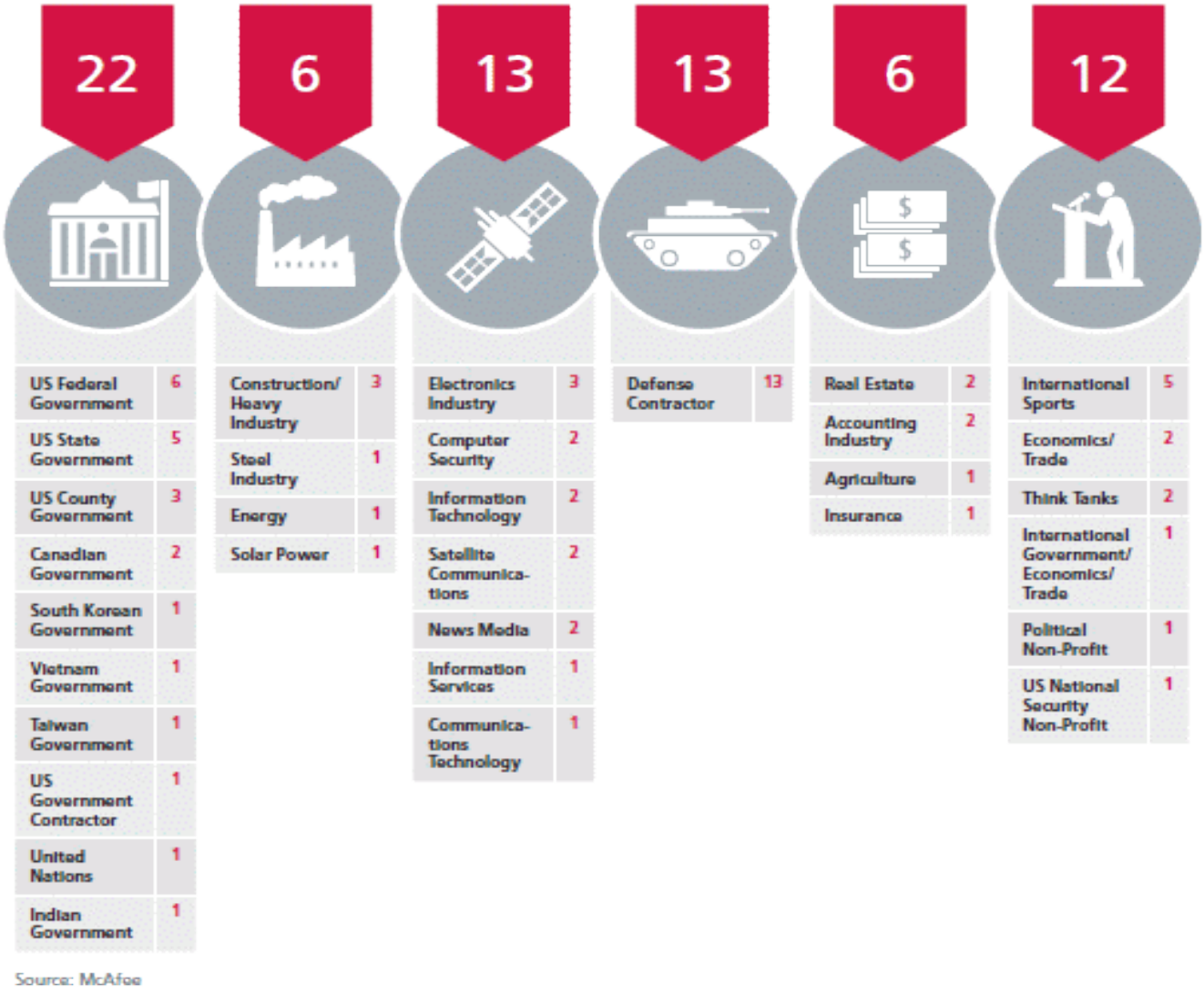
2.3.2.6 Shady RAT

McAfee hat im März 2011 den Zugang zu den Logfiles eines schon 2009 entdeckten Command and Control Servers – C&C – erlangt, den hungrige Datendiebe bereits seit 2006 als Sprungbrett zu den Datenbanken von insgesamt 72 weltweit verteilten Unternehmen und Organisationen nutzen. Ihre Methode ist einfach und fast schon klassisch zu nennen: Die Angreifer senden an die Mitarbeiter ausgesuchter Unternehmen ("Spear-Phishing") E-Mails mit Anhängen, die eine Download-Routine enthalten. Damit wird die Malware geladen, die eine Hintertür (Backdoor) für den C&C öffnet und den Angreifern den Zugang gibt [108].

Den schon lange dauernden Angriff nennt McAfee "Operation Schattige Ratte", was sich aus dem englischen Sprachgebrauch ableitet, Programme zum Fernzugriff auf fremde Systeme als Ratten (Remote Access Service – RAS ~ Rats) zu bezeichnen. Betroffen sind 72 Organisationen, *darunter ... die ... Regierungen Indiens, Kanadas, Taiwans, Südkoreas, Vietnams und der USA,* <das> *IOC,* <die> *Vereinten Nationen, ... ASEAN oder* <die> *Antidoping-Behörde sowie ... Hightech-Unternehmen und Rüstungsfirmen, Thinktanks und*

---

[108] Dmitri **Alperovitch**, Revealed: Operation Shady RAT, McAfee 05.08.2011, S. 3, 4.
Auch die Grafik auf der Folgeseite stammt aus dem Bericht.



Medien [109]. Die Menge der ausgespähten Daten wird in Petabytes geschätzt, also in einer Größenordnung, in der Sony weltweit über Speicherplatz für Videos verfügt [110].

Die Qualität der ausgespähten Daten ist unbekannt, was angesichts der schieren Menge auch unbedeutend ist: Alles, was an Interna und Geheimnisse greifbar ist.

Ungewöhnlich ist: Die Operation dauert schon seit 5 Jahren an und ist kein lockerer Hack, der mal eben zum Spaß durchgeführt wird. Bei der Auswahl der Opfer konzentrieren sich die Angreifer auf Nordamerika (53), Europa ist kaum betroffen (6), etwas stärker der Ferne Osten (8) [111]. Die Dauern der Angriffe sind teilweise kurz und in anderen Fällen reichen sie über Jahre hinweg [112]. Die Ziele als solches lassen kein spezifisches Muster und keinen Schwerpunkt erkennen [113]. Das unterscheidet sie von den Angriffen unter ▸ Aurora vom Anfang 2010.

Die Angreifer scheinen an den Informationen als solche interessiert sein. Es sind keine Erpressungsversuche bekannt geworden. Das spricht für Industrie- und andere Spionage. Deshalb vermutet McAfee die Angriffe aus Russland oder China stammend. Tatsächlich sind beide Länder nicht

[109] Florian **Rötzer**, Bislang größte Cyberhack-Serie entdeckt, Telepolis 03.08.2011

[110] **CF**, IT in Zahlen, 08.04.2011

[111] McAfee, ebenda, S. 5.

[112] McAfee, ebenda, S. 9 bis 13.

[113] McAfee, ebenda, S. 7 bis 8.

von ihnen betroffen, wohl aber Südkorea und Taiwan (jeweils 3), Indonesien, Singapore und Hong Kong (je 1). Das lässt eher eine chinesische Handschrift vermuten. Die verwendete Angriffstechnik ist technisch betrachtet solides Handwerk. Ihr fehlt aber das handwerkliche Niveau jüngster Angriffe, mit dem zum Beispiel beim ▸ Night Dragon vorgegangen wurde.

Einzigartig ist hingegen die kaum noch begreifbare Datenmenge, die hier abgegriffen wurde, und die lange Zeit, über die die Aktion lief. Der Zeitfaktor spricht dafür, dass die Angreifer die Daten nicht einfach nur abgesogen, sondern auch in ganzer Tiefe ausgewertet haben.

2.3.3 Malware und IuK-Strafrecht

Das Beispiel von ▸ Aurora zeigt uns anschaulich die Schritte, mit denen sich die Malware einnistet und schließlich ihre schädlichen Funktionen ausführt:

❶ Anlieferung

❷ Injektion

❸ Infektion

❹ Einnisten

❺ Tarnen

❻ Malware ausführen

Besonders die ersten vier Schritte des völlig automatisierten Prozesses (siehe ▸ Malware ... und ▸ Aurora) interessieren für die Frage, ob damit bereits eine Computersabotage (§ 303b StGB) oder ein Ausspähen von Daten (§ 202a Abs. 1 StGB) vollendet wird. Für beide Strafvorschriften gilt, dass sie einen Unrechtserfolg voraussetzen, der einerseits in der Zerstörung von Daten und andererseits in ihrer unberechtigten Wahrnehmung (Ausspähen, Abfangen) besteht. Ein menschliches Zutun bei der Vollendung verlangen sie nicht, so dass als Tathandlung das noch im Vorbereitungsstadium angesiedelte Einrichten von Webseiten oder Präparieren von E-Mails mit Malware als komplettes Programm oder von Startern ausreicht, die den automatischen Download der Malware initiieren sollen [114].

Dieser Abschnitt betrachtet zunächst nur die Installation von Malware und nicht auch ihre Auswirkungen.

---

[114] Dieses Vorgehen wird schon lange unter dem Begriff Pharming diskutiert (**CF**, Pharming, 2007), wobei die Täter eine Vielzahl von nachgemachten Bankenseiten präsentieren, auf die sie die Kunden verschiedener Banken locken, zu unbedarften Dateneingaben überreden oder von dort schädlichen Code zuspielen. Eine Abwandlung davon besteht darin, dass durch viele miteinander verlinkte Webseiten und die Verwendung häufig nachgefragter Suchworte beste Platzierungen bei den Suchmaschinen erreicht und dadurch die Anwender angelockt werden. Schließlich werden auch die Webserver von frequentierten Angeboten angegriffen und so manipuliert, dass sie die Malware verbreiten.

2.3.3.1 Datenveränderung, Computersabotage

Die Vorschrift über die Datenveränderung (§ 303a Abs. 1 StGB) hat ihren Ursprung im Recht der Sachbeschädigung. Das zeigt sich auch daran, dass erst die zerstörerische Veränderung unter Strafe gestellt ist: Bestraft wird, wer *Daten ... löscht, unterdrückt, unbrauchbar macht oder verändert*. Daraus folgt, dass eine merk- oder messbare Veränderung im Datenbestand hervorgerufen werden muss. Das ist jedenfalls bei der Anlieferung und Injektion noch nicht der Fall. Zur Infektion werden zunächst nur ungesicherte Umgebungsfunktionen dazu genutzt, um die Malware zu installieren. Entscheidend dafür, ob bei der Infektion Daten verändert werden, ist die Methode, die dazu verwendet wird. Eine besteht darin, den Arbeitsspeicher zu perforieren („Tu-nix-Rutsche“ [115]). Dabei können andere Daten, die den Ablauf des Computers bestimmen, überschrieben und gelöscht werden. Sie werden aber nicht unwiederbringlich gelöscht und eine Störung im Sinne von § 303a Abs. 1 StGB ist bei der Infektion eher nicht zu erwarten, sondern erst beim Einnisten selber, wenn dabei Systemdateien nicht nur erweitert, sondern abgeändert und überschrieben werden.

Deshalb ist es eine Frage des Einzelfalls, ob vor der Installation einer Malware auch eine Datenveränderung eintritt. Das ist spätestens dann der Fall, wenn bei der Tarnung Virenscanner abgeschaltet oder andere Sicherheitsvorrichtungen manipuliert werden. Auch die Einrichtung einer Backdoor verändert zwangsläufig Daten.

Die Computersabotage setzt einen Schritt früher an und droht dem mit Strafe, wer *Daten ... in der Absicht, einem anderen Nachteil zuzufügen, eingibt oder übermittelt* (§ 303b Abs. 1 Nr. 2 StGB). Sie stellt bereits die Injektion als Übermittlung von Daten unter Strafe, wobei die Tat mit der Injektion vollendet ist, weil es hier, anders als bei § 303a StGB, der einen zerstörerischen Erfolg zur Vollendung voraussetzt, nur auf die Absicht des Täters ankommt, mit der Malware eine erhebliche Störung zu bewirken [116].

Allerdings müssen für § 303b Abs. 1 StGB zwei weitere Voraussetzungen erfüllt sein: Die angegriffene Datenverarbeitung muss für einen anderen von wesentlicher Bedeutung und die Störung muss erheblich sein. Mit dieser seit 2007 geltenden Wortwahl hat der Gesetzgeber auch die private Nutzung der Informationstechnik unter den Schutz der Computersabotage gestellt, wobei er nur die ***Bagatelltechnik*** ausgenommen hat, also vor allem einfache Taschenrechner oder die Steuerungen für Haushaltsgeräte.

Meine weite Auslegung des Merkmals „wesentliche Bedeutung“ wird unterstützt von den Ausführungen des BVerfG im Zusammenhang mit der Onlinedurchsuchung: *Die Leistungsfähigkeit derartiger Rechner ist ebenso gestiegen wie die Kapazität ihrer Arbeitsspeicher und der mit ihnen verbundenen Speichermedien. Heutige Personalcomputer können für eine Vielzahl unterschiedlicher Zwecke genutzt werden, etwa zur umfassenden Verwaltung und Archivierung der eigenen persönlichen und geschäftlichen Angelegenheiten, als digitale Bibliothek oder in vielfältiger Form als Unterhaltungsgerät. Dementsprechend ist die Bedeutung von Personalcomputern für die Persönlichkeitsentfaltung erheblich gestiegen* [117].

Aus der verfassungsrechtlichen Sicht sind damit grundsätzlich alle handelsüblichen Computer Gegenstände, die dem privaten Integritätsschutz unterliegen und das besonders dann, wenn sie vernetzt sind. Die Grenze dazu setzt das BVerfG sehr flach: Systeme, die von ihrer Technik her *lediglich Daten mit punktuellem Bezug zu einem bestimmten Lebensbereich des Betroffenen* verarbeiten, *zum Beispiel nicht vernetzte elektronische Steuerungsanlagen der Haustechnik*, vermitteln noch

---

[115] Thorsten **Holz**, Alarm beim Pizzadienst, c't 13/2010, S. 184

[116] Daneben regelt § 303b Abs. 5 StGB unter Bezugnahme auf § 202c StGB ausdrücklich eine Strafbarkeit im Vorbereitungsstadium.

[117] **BVerfG**, Urteil vom 27.02.2008 - 1 BvR 370/07, 595/07, Rn 172;
weitere Einzelheiten: **CF**, informationstechnische Systeme, 05.04.2008.

keinen Integritätsschutz [118].

Mit der Forderung nach einer gewissen Erheblichkeit grenzt sich § 303b Abs. 1 StGB gegen ***Bagatellschäden*** ab, wobei nach den Auswirkungen der Malware zu fragen ist (Erfolg). Dazu muss die Qualität der Daten und der Datenverarbeitung betrachtet werden, gegen die sich die Malware richtet. Wenn, wie bei Aurora, eine Backdoor eingerichtet werden soll, um dadurch Zugriff auf Unternehmensgeheimnisse zu erlangen, steht die Erheblichkeit außer jedem Zweifel. Das gilt bei privaten Zwecken sicher auch dann, wenn Phishing-Malware gegen das Onlinebanking oder Handelsvorgänge eingebracht wird, wenn handelsfähige Werte zerstört werden (Musik- oder Fotosammlungen) und schließlich wegen der Daten mit persönlichem Bezug (Archive: familiäre Datensammlungen, Tagebücher, Korrespondenz, Datensammlungen und Schriftverkehr zu Steuererklärungen, Versicherungen und Alltagsgeschäften). Das würde auch für vorübergehende Beeinträchtigungen gelten, die von Ransomware ausgelöst werden [119]. Danach bleibt für Bagatellschäden im Sinne von § 303b Abs. 1 StGB allenfalls eine Art Bodensatz aus überalterten, kaum genutzten PCs und verpackungsfrischen Neugeräten.

Das lässt folgende Schlüsse zu:

- Schon handelsübliche Haushaltscomputer und mit ihnen verbindungsfähige Zusatzgeräte (Mobiltelefone, Organizer), die private Daten aufnehmen und verwalten, sind grundsätzlich für einen anderen von wesentlicher Bedeutung und unterliegen dem Schutz des § 303b Abs. 1 StGB (Computersabotage).

- Die Computersabotage ist bereits mit der Anlieferung der Malware, spätestens mit der Infektion vollendet, weil das Tatbestandsmerkmal der Übermittlung die schädigende Handlung in das Vorbereitungsstadium verlagert, ohne dass es eines Schadens als Erfolg bedarf. Auf die Absicht kommt es an, also darauf, welche schädigende Wirkung mit der Malware ausgelöst werden soll. Insoweit ist das „Übermitteln“ im Sinne von § 303b Abs. 1 Nr. 2 StGB etwas strenger wegen des erstrebten Erfolges auszulegen als die den Erfolg bereits vorausetzenden Tatbestände des § 303a StGB, die auch ungewollte, aber vorhersehbare Schäden umfassen [120].

Bereits der Versuch der Datenveränderung und der Computersabotage ist strafbar (§§ 303a Abs. 2, 303b Abs. 3 StGB). Beide verlangen wegen ihrer Grundtatbestände nach einem Strafantrag, wenn nicht die Staatsanwaltschaft das besondere öffentliche Interesse an der Strafverfolgung erklärt (§ 303c StGB [121]).

Das gilt nicht für die besonders schweren Fälle der Computersabotage (§ 303c Abs. 4 StGB), die bei großen Vermögensverlusten, öffentlichen Versorgungsengpässen und Sicherheitsgefahren sowie beim gewerbs- oder bandenmäßigen Handeln greifen. Während der Gesetzgeber die Grundtatbestände im Bereich der leichten Kriminalität ansiedelt, betrachtet er die besonders schweren Fälle als schwere Kriminalität, die im Einzelfall mit bis zu zehn Jahren Freiheitsstrafe bestraft werden können. Das ist ein ganz deutlicher Unterschied [122].

---

[118] BVerfG ebenda, Rn 202.

[119] Ransomware (auch Scareware) ist eine Malware, die die Daten auf einem angegriffenen System verschlüsselt und erst gegen Schutzgeld wieder freigeschaltet werden können. Das strafrechtliche Ergebnis ihres Einsatzes ist eine Erpressung (§ 253 StGB), häufig gepaart mit einem Betrug (§ 263 StGB), wenn statt eines speziellen Virenscanners ein unnützes „Fake“programm oder weitere Malware übermittelt wird. Grundlegend zum Thema: François **Paget**, Angst einjagen und abkassieren: Mit vorgeblicher Sicherheits-Software wird weltweit viel Geld ergaunert, McAfee 03.12.2010; Abhishek **Karnik**, Avelino C. **Rico**, Jr., Amith **Prakash**, Shinsuke **Honjo**, Identifying Fake Security Products, McAfee 16.12.2009.

[120] Bedingter Vorsatz: Der Täter will nicht den schädlichen Taterfolg erreichen, kennt aber die Möglichkeit, dass er eintritt und nimmt ihn billigend in Kauf.

[121] Auslegungshilfe im Zusammenhang mit dem besonderen öffentlichen Interesse: Nr. 86 Abs. 2 RiStBV. Es handelt sich um keine Privatklagedelikte im Sinne von § 374 StPO.

[122] Man sollte erwarten, dass sich die schwere Kriminalität im ▸ Straftatenkatalog des § 100a Abs. 2 StPO wider spiegelt. Dort ist die besonders schwere

2.3.3.2 Ausspähen von Daten

Der in § 202a Abs. 2 StGB bestimmte Datenbegriff behandelt die Daten inhaltlich neutral und macht keinen Unterschied zwischen allgemeinen, persönlichen oder sogar sensiblen Dateninhalten. Die Strafvorschrift des § 202a Abs. 1 StGB schränkt den Schutzbereich ein, weil die betreffenden Daten besonders geschützt sein müssen und das Ausspähen gerade unter Überwindung dieser Zugangssicherung erfolgen muss. Das verlangt, dass über die einfache Speicherung *hinaus Vorkehrungen getroffen sein müssen, die den unbefugten Zugriff auf Daten ausschließen oder zumindest erheblich erschweren* [123].

Im Vergleich zum Ausspähen von Daten fällt auf, dass § 202b StGB zwei einschränkende Stufen formuliert: Es muss sich um Daten handeln, die nicht für den Täter bestimmt sind, und er muss sie sich entweder *aus einer nichtöffentlichen Datenübermittlung oder aus der elektromagnetischen Abstrahlung einer Datenverarbeitungsanlage* verschaffen.

Bei der Übermittlung fallen verschiedene Daten an, die sich an unterschiedliche Adressaten richten. Für die Zugangsprovider und Carrier sind die Protokoll- und Adressdaten bestimmt, ohne die weder die Telefonvermittlung noch das Routing [124] nach dem Internetprotokoll die aussagekräftigen Inhalte zielgerichtet [125] und vollständig [126] transportieren könnten.

Die Inhaltsdaten richten sich hingegen an den bestimmten Adressaten und eben nicht an eine unbestimmte Öffentlichkeit. Entsprechend spricht das TKG genauer von der „Meldung“ und unterwirft sie einem Abhör- und Weitergabeverbot (Funkschutz, § 148 Abs. 1 Nr. 1 TKG). Für die Telekommunikation macht das Abfangverbot deshalb nur dann einen Sinn, wenn man davon ausgeht, dass die mit einer Meldung verbundenen Verkehrsdaten zwischen den Endgeräten zwar an öffentlich tätige Zugangsprovider gerichtet sind, nicht aber die Meldung als solche, die die Inhaltsdaten enthält.

Auch das Abfangen von Verkehrsdaten auf öffentlichen Übertragungsstrecken ist von § 202b StGB erfasst. Das Routing in den kabelgebundenen Telekommunikationsnetzen ist zwar variabel, gehorcht aber technischen und wirtschaftlichen Zwecken. Es ist kein öffentlicher (beliebiger), sondern geschlossener Vorgang, an dem nur die Zugangsprovider und Carrier beteiligt sind. In den lokalen Netzen „hinter“ den Endgeräten ist auch der Übermittlungsvorgang zweifellos nichtöffentlich. Als öffentliche Übertragungsmedien kommen im Ergebnis nur kabellose in Betracht, also im wesentlichen der Funk.

Diese Einschätzung wird davon unterstützt, dass neben der „nichtöffentlichen Datenübermittlung“ auch die „Abstrahlung“ geschützt ist. Dabei handelt es sich um die elektromagnetischen Emissionen, die von Bildschirmen, Kabelverbindungen und elektronischen Bauteilen ausgehen und aus denen (mit aufwändiger Technik) eine Meldung oder Fragmente von ihr herausgefiltert werden können. Diese Alternative belegt, dass der Gesetzgeber die technischen Zugriffsmöglichkeiten vor Augen hatte, die mit der regulierten Telekommunikation normalerweise nicht erreicht werden.

Computersabotage aber nicht aufgeführt.

[123] **BGH**, Beschluss vom 14.01.2010 – 4 StR 93/09, S. 4 (Skimming).

[124] Zielgerichtete Netzdurchleitung - Routing.

[125] Gemeint ist die genaue Verbindung zwischen mindestens zwei protokollarisch definierten Endpunkten.

[126] Die Vollständigkeit spricht die Besonderheiten der paketorientierten Übermittlung an (Transmission Control Protocol - TCP). Bei ihr werden die Inhalte auf eine Vielzahl von kleinen Informationspaketen verteilt, die über verschiedene Strecken zum Zielpunkt gelangen können. Hier müssen sie wieder in die richtige Reihenfolge gebracht, zusammengeführt und verloren gegangene Pakete nachgefordert werden. Das setzt voraus, dass alle Informationspakete jedenfalls vorübergehend bis zum vollständigen Abschluss des Übermittlungsvorganges zwischengespeichert werden (Cashing). Dabei handelt es sich um eine andere Art der Zwischenspeicherung als die, die von § 9 TMG angesprochen wird. Das TCP sichert die Übermittlung als solche und das TMG ermöglicht die schnelle Bereitstellung derselben Inhalte an eine Mehrzahl von Berechtigten.

Für die Auslegung des § 202a Abs. 1 StGB folgt daraus, dass jedenfalls aus dem systematischen Zusammenhang der korrespondierenden Vorschriften über das Ausspähen und Abfangen von Daten keine besonderen Anforderungen an den Inhalt von „Meldungen“ und Daten abzuleiten sind.

Daraus, dass sich beide Vorschriften in dem Abschnitt über die Verletzungen des persönlichen Lebens- und ***Geheim***bereichs befinden, ergeben sich ebenfalls keine einschränkenden Anforderungen an die inhaltliche Qualität. Auch die einleitende Strafnorm zur Vertraulichkeit des Wortes (§ 201 StGB) wendet sich nur gegen die heimliche technische Aufzeichnung des gesprochenen Wortes und seine technische Wiedergabe. Einen inhaltlichen Wert verlangt schließlich nur § 274 StGB für technische Aufzeichnungen und beweiserhebliche Daten, die wie andere Urkunden einen Aussagewert haben müssen (Aussteller, rechtsgestaltende Aussage). Ihre Vernichtung oder Unterdrückung kann mit Freiheitsstrafe bis zu fünf Jahren geahndet werden.

Damit bleiben aus dem allgemeinen Schutzbereich des Datenschutzrechts der §§ 202a, 202b StGB nur zwei wesentliche Einschränkungen übrig:

- Die Daten dürfen nicht für den Späher bestimmt sein und
- darüber hinaus müssen sie über punktuelle Aspekte des persönlichen Lebensbereiches hinausgehende Aussagen ermöglichen.

Internetbrowser sind gesprächig und vermitteln der Gegenstelle Auskünfte über sich selber (Programm und Version), über die Plattform, auf der sie betrieben werden (zum Beispiel Windows und Version), und über den Zugangsprovider, den sie nutzen. Daraus lässt sich auch die regionale Herkunft des Anwenders abschätzen. Diese Daten werden unkontrolliert an jeden Kommunikationspartner verteilt und sind deshalb öffentlich. Sie reichen für die Injektion durch infizierte Webseiten aus, so dass jedenfalls bei diesem Angriffsschritt grundsätzlich noch kein Ausspähen oder Abfangen von Daten in Frage kommt.

Diese Daten gehen bereits über punktuelle Aspekte der privaten Lebensgestaltung hinaus und geben klare Auskünfte über den Anwender. Am wichtigsten ist die Region, aus der er stammt. Daraus lassen sich die Sprache, die er spricht, die Tastaturbelegung, die er nutzt, und regionale Besonderheiten abschätzen, die auf ihn zutreffen dürften (die Bewohner Hamburgs oder anderer deutscher Großstädte nagen wahrscheinlich nicht am Hungertuch und lassen finanzielle Beute erwarten). Aus der Art des Browsers lässt sich ableiten, ob der Anwender Standardprogramme nutzt, ohne sich tiefere Gedanken über alternative Programme zu machen (mit Windows wird der entsprechende Explorer installiert), oder tiefere Kenntnisse hat, die methodisch generalisierte Angriffe vereiteln könnten. Aus der Aktualität des Betriebssystems lässt sich auf die prinzipielle Zahlungskraft des Nutzers schließen (er gibt Geld für ein neues System aus) und aus der Aktualität von Betriebssystem und Browser darauf, ob er sein System aktualisiert oder schluren lässt.

Dieser Ausflug in das Social Engineering belegt, dass bereits aus drei belanglos scheinenden Informationen durch fachkundige Interpretation eine noch allgemeine, aber brauchbare Persönlichkeitsstudie abgeleitet werden kann [127]. Daran anknüpfend ist zu fragen, ob auch rein informationstechnisch und automatisch generierte Daten geschützte Daten im Sinne von § 202a Abs. 1 StGB sind.

Im Telekommunikationsrecht wird insoweit zwischen dem Abhören (Überwachung der Telekommunikation, § 100a StPO) und dem Zugriff auf Verkehrsdaten (§ 100g StPO) unterschieden. Das Abhören bezieht sich auf den Inhalt der Kommunikation, also auf die Meldung im Sinne des Abhörverbots im TKG. Die Verkehrsdaten geben hingegen Auskunft über die begleitenden Umstände der

[127] Für das Social Engineering gilt, dass aus ***fünf*** unverfänglichen Informationen eine brisante abgeleitet werden kann. Wenn ich eine Pharm aufbaue, mit der ich ganz verschiedene Bankkunden anlocke, dann bekomme ich die vierte Information: Du bist Kunde bei einer bestimmten Bank. Daraus lassen sich weitere Schlüsse ziehen.

Telekommunikation, also wer mit wem (Anrufer und Angerufener), wo (stationäres Endgerät, Standortdaten) und wie lange kommuniziert hat. Beide, Inhalts- und Verkehrsdaten, werden von Art 10 GG geschützt [128], obgleich die Eingriffstiefe bei der Überwachung der Telekommunikation ungleich tiefer ist als beim Zugriff auf Verkehrsdaten (was gelegentlich in Vergessenheit gerät). Aus den Verkehrsdaten lässt sich auf das Kommunikationsverhalten des Betroffenen schließen, sie geben Auskunft über seine Kommunikationspartner, die Dauer der Kommunikation und ihre Häufigkeit. Daraus lässt sich ein persönliches Profil mit Aussagewert erstellen, umso mehr, wenn auch die Standortdaten einbezogen werden (§ 98 TKG, § 100g Abs. 1 S. 3 StPO), aus denen sich ein Bewegungsprofil erstellen lässt.

Die Verkehrsdaten werden zwar automatisch generiert, die Veranlassung dazu geben aber menschliche Handlungen, also die Tatsache, dass Menschen miteinander telefonieren. Aus der verfassungsrechtlichen Diskussion ist mir kein Beispiel geläufig, dass zwischen der menschlich-willentlichen und einer automatisch veranlassten Kommunikation (Spam-Mails, Standortmeldungen von Pkws) unterschieden würde, wobei durchaus ein Unterschied besteht, weil Automaten (noch) keine Grundrechte haben. Sie vermitteln aber auch Auskünfte über menschliches Handeln, schwache im Zusammenhang mit Spam-Mails (es gibt einen Menschen, der den Vorgang geplant und gestartet hat) und ziemlich starke wegen der Standortmeldungen mancher Pkws (ein Mensch fährt das Fahrzeug und befindet sich jetzt an dem und dem Ort). Auch die Standortdaten im übrigen werden automatisch generiert und unterliegen fraglos dem Grundrechtsschutz, weil sie Auskunft über die Bewegungen des Handy-Trägers geben.

Das Telekommunikationsverwaltungsrecht behandelt persönlich und automatisch generierte Daten ebenfalls gleich (§ 3 Nr. 22 TKG).

Daraus folgt nach grammatischer, systematischer und verfassungskonformer Auslegung, dass der Datenbegriff des § 202a Abs. 2 StGB keinen Unterschied zwischen verschiedenen inhaltlichen Qualitäten macht, sondern nur danach fragt, an wen die Daten gerichtet sind, ob sie gegen das Ausspähen besonders geschützt sind und ob das Abfangen irregulär erfolgt. Selbst automatisch generierte Daten unterliegen diesem Schutz, wenn sie irgendeine Aussage über den Betreiber oder Anwender der Informationstechnik geben.

Übertragen auf den Angriffsablauf bei ▸ Aurora folgt daraus, dass jedenfalls die Injektion der Malware über Automatiken in Webseiten kein Ausspähen oder Abfangen von Daten ist, wenn zwar Umgebungsvariablen missbraucht werden, diese aber von den Browsern oder anderen Anwenderprogrammen mit Netzanbindung freimütig (öffentlich) zur Verfügung gestellt werden. Sobald die Malware aber bei der Infektion und ihrer Installation ihre Nistumgebung erkundet, späht sie Daten aus und ist § 202a Abs. 1 StGB vollendet, weil es nicht darauf ankommt, wer die Daten generiert hat, sondern nur darauf, ob sie öffentlich präsentiert oder durch Schutzvorrichtungen separiert sind.

Dieses Ergebnis offenbart ein Schutzprinzip, das auch für öffentliche informationstechnische Geräte wie Webserver, Router und Mailserver gilt. Ihre Netzfunktion ist öffentlich – also ihr oberflächlicher Ereignishorizont – und kann durch übliche Werkzeuge erfragt werden (Ping, Tracerouting, Sniffer, soweit sie von außen agieren). Ihr Inneres, ihre von außen nicht zugängliche Konfiguration und ihre Administration sind nicht für die Öffentlichkeit bestimmt und deshalb dem Geheimnisschutz unterworfen. Zugelassen sind auch trickreiche Anfragen (Sniffer), die vielleicht mehr Informationen aus dem System locken, als der Betreiber will, weil ihnen kein Schutzmechanismus entgegen gestellt wurde, solange diese Informationen protokollgerecht (TCP-Familie, ISO) abgefragt werden. Sobald aber Sicherheitslücken durch aktive Steuerungen missbraucht werden, unterliegen die dadurch gewonnenen Daten dem strafrechtlichen

[128] **BVerfG**, Urteil vom 27.02.2008 - 1 BvR 370/07, 595/07, Rn 182, 183, 184 (Onlinedurchsuchung)

Datenschutz [129].

2.3.3.3 Vorbereitungshandlungen

Als strafbare Vorbereitungshandlungen hat der Gesetzgeber im IuK-Strafrecht vorgesehen:

- Der Umgang [130] mit Kartenlesegeräten (Skimmer) als Computerprogramme oder ähnliche Vorrichtungen, die zur Fälschung von Zahlungskarten genutzt werden sollen (§§ 152a Abs. 5, 152b Abs. 5 i.V.m. 149 Abs. 1 Nr. 1 StGB) [131].

- Der Umgang mit Passwörter oder sonstige Sicherungscodes, die den Zugang zu Daten ermöglichen (§ 202c Abs. 1 Nr. 1 StGB). Gemeint sind alle Zugangsdaten zu Accounts, die dem strafrechtlichen Datenschutz der §§ 202a und 202b StGB (▸ Ausspähen von Daten) sowie zur Vorbereitung der ▸ Computersabotage (§§ 303a Abs. 3, 303b Abs. 5 StGB) unterliegen. Das führt dazu, dass zwar die „Datenhehlerei“ straflos ist, also der Handel mit ausgespähten oder anderweitig gestohlenen Daten, nicht aber der Handel mit Zugangsdaten (Verschaffen, Verkaufen, Überlassen). Danach ist auch das unberechtigte Herstellen von Zugangsdaten beim Cracking [132] verboten. Handelt es sich um urheberrechtlich und technisch geschützte Zugangssicherungen, greift die besondere Vorschrift des § 108b Abs. 1 Nr. 1 UrhG.

- Der Umgang mit Computerprogrammen, deren Zweck das Ausspähen oder Abfangen von Daten (§ 202c Abs. 1 Nr. StGB), die Computersabotage (§ 303b Abs. 5 StGB) oder der Computerbetrug ist (§ 263a Abs. 3 StGB).

Nur § 149 StGB droht mit einer Freiheitsstrafe bis zu fünf Jahren (mittlere Kriminalität), § 263a Abs. 3 StGB mit höchstens drei Jahren Freiheitsstrafe und die übrigen mit einem Jahr (leichte Kriminalität). Verdeckte und andere intensive Ermittlungen lässt allenfalls § 149 StGB zu [133].

Den Kontroversen um den Hackerparagraphen (§ 202c StGB) hat das BVerfG ein Ende gesetzt [134], indem es den gesetzgeberischen Willen in Erinnerung gebracht hat <Rn 60>: *Tatobjekt des § 202c Abs. 1 Nr. 2 StGB kann nur ein Programm sein, dessen Zweck die Begehung einer Straftat nach § 202a StGB (Ausspähen von Daten) oder § 202b StGB (Abfangen von Daten) ist. Danach muss das Programm mit der Absicht entwickelt oder modifiziert worden sein, es zur Begehung der genannten Straftaten einzusetzen. Diese Absicht muss sich ferner objektiv manifestiert haben.* Es reicht nicht, dass ein Programm einfach nur zum kriminellen Zweck geeignet ist <Rn 61>. In ihm muss sich eine kriminelle Absicht manifestieren <Rn 67>, so dass handelsübliche Vorrichtungen und Programme, die ***auch*** zu Straftaten genutzt werden können (Dual Use), nicht strafbar sind.

Dieses Prinzip habe ich im Zusammenhang mit dem Skimming auch auf die zum Computerbetrug bestimmten „Programme“ angewendet (§ 263a Abs. 3 StGB), was dazu führt, dass handelsübliche Digitalkameras und Mobiltelefone, die in Attrappen für das Ausspähen von PIN verbaut werden, zwar geeignete, aber keine zum Computerbetrug bestimmten Bauteile sind, solange ihre

---

[129] Diese Einschränkung folgt dem Grundgedanken, den der 1. Strafsenat des BGH im Zusammenhang mit dem Ausspähen von Daten bei Skimminggeräten aufgebracht hat: Wenn nicht handelsübliche und teure Geräte eingesetzt werden, die dazu geeignet sind, die besonders stark magnetisierten Spuren 1 und 2 von Zahlungskarten zu überschreiben, dann könnte wieder von einem Zugangsschutz ausgegangen werden, der eben durch diese Geräte überwunden wird. Siehe:
BGH, Beschluss vom 19.05.2010 - 1 ARs 6/10.

[130] „Umgang“ ist ein Begriff aus dem Waffenrecht und bezeichnet verschiedene Ausformungen des tatbestandlichen Handelns wie das Herstellen, Anbieten, Verbreiten, Verschaffen usw. Ich verwende den Begriff ebenfalls, um umständliche Wiederholungen der Tatbestandsvarianten zu vermeiden.

[131] Wenn die Geräte nur zu Fälschung geeignet sind, die persönliche Absicht zur Fälschung aber nicht bewiesen werden kann: Ordnungswidrigkeit gemäß § 127 OWiG.

[132] Kopierschutz: Crack (Software); Brute-Force-Methode.

[133] Dieter **Kochheim**, Verdeckte Ermittlungen im Internet, 27.07.2011

[134] **BVerfG**, Beschluss vom 18.05.2009 - 2 BvR 2233/07

Steuerung nicht verändert wird [135].

Bezogen auf die Installation verschiedener Malwareformen greifen auch die strafbaren Vorbereitungshandlungen, ohne dass auch der strafbare Erfolg eintreten muss:

▸ ***Pharming***: Das Einrichten und vor allem das Betreiben von präparierten Webseiten bereitet sowohl das Ausspähen und Abfangen von Daten als auch die Computersabotage vor (§§ 303a Abs. 3, 303b Abs. 5 StGB). Diese Tathandlungen sind jedenfalls mit dem Einsatz von Malware für das Onlinebanking und für Botnetze verbunden. Sobald sich die Malware einnistet (installiert), ist der Grundtatbestand verwirklicht und das Vorbereitungsstadium abgeschlossen.

Wegen des Pharmings und der unten angesprochenen Malwareformen ist der ▸ Rückruftrick in Erinnerung zu rufen: Hier wie dort handelt der Täter nur einmal, wenn er seine technischen Fallen aufbaut. Dabei hat er eine bestimmte Vorstellung von dem Opfertyp, weil er spezifische technische Methoden einsetzt, um bestimmte Schwachstellen zu überwinden (Exploits), die nur genau definierte Betriebssysteme oder Anwenderprogramme unterlaufen können, und mit Texten und Gestaltungen arbeitet, die auf bestimmte Anwendertypen abgestimmt sind. Alles weitere überlässt er dem Zufall. Das bedeutet, dass ein aktives Täterhandeln nicht mehr erforderlich ist, um den strafrechtlichen Taterfolg zu erreichen. Alle Einzelschäden, die die Malware – auch im Zusammenspiel mit einem automatisierten C&C-Server – dann anrichtet, ist aus der Sicht des Täters nur eine einheitliche prozessuale Tat, so dass die isolierte Strafverfolgung zum Strafklageverbrauch wegen der nicht betrachteten Schäden führt. Erst wenn der Täter die Malware aktualisiert, eine neue Spam-Welle startet oder die Zielgruppe verändert oder präzisiert, beginnt er eine neue Tatserie.

Das hat für die Strafverfolgung eine unangenehme Konsequenz: Sie darf sich nicht auf den einzelnen Schadensfall beschränken, sondern muss die Schadensakte zusammenfassen, um die einzelnen Täterhandlungen voneinander abzugrenzen. Wichtige Faktoren dabei sind die Zeitpunkte, ab wann zum Beispiel eine Spam-Kampagne aufgetreten ist, wann ihr die nächste folgte und ob dabei Varianten der Malware zum Einsatz kamen. Das erfordert eine qualifizierte und auch technisch fachkundige Ermittlungsarbeit.

▸ ***PIN-Skimming***: Die Module, die jetzt in POS-Terminals verbaut werden, um im Einzelhandel die Kartendaten vom EMV-Chip und die Eingabe der PIN abzugreifen, sind wegen ihrer auf das Skimming abgestimmten Programme sowohl im Sinne von § 149 Abs. 1 Nr. 1 und § 263a Abs. 3 StGB als auch als sonstige (technische) Vorrichtungen zum Fälschen von Zahlungskarten im Sinne von § 149 Abs. 1 Nr. 1 StGB strafbar.

Bei ▸ ***Trojaner-Baukästen*** muss nach ihrem Funktionsumfang gefragt werden. Soll die geplante Malware als Botware verwendet werden, handelt es sich um Computerprogramme zur Datenspionage und Computersabotage (siehe oben). Diese Tathandlungen werden bereits bei der Installation ausgeführt und einmal mehr, wenn die Malware auch persönliche Daten wie Kontenzugangsdaten oder Lizenzschlüssel ausspäht und an den Betreiber meldet.

▸ ***Onlinebanking-Trojaner*** haben nicht nur tatsächlich komplizierte Funktionen, sondern lassen sich auch rechtlich nur schwer handhaben. Im Vorgriff auf spätere Erörterungen ist zu sagen, dass sie im wesentlichen zum Computerbetrug bestimmt sind. Somit handelt es sich bei den Trojanern und den C&C-Servern um den Einsatz von Computerprogrammen, die speziell zum Computerbetrug eingerichtet und betrieben werden, so dass im wesentlichen dafür Strafe nach § 263a Abs. 3 StGB droht.

▸ ***Ransomware*** ist dazu bestimmt, die Funktionen der angegriffenen Geräte zu stören oder schlimmer noch: abzuschalten. Sie sind Computerprogramme, die ausdrücklich zur Computersabotage bestimmt sind.

Der ▸ ***Handel mit ausgespähten Zugangsdaten*** ist ein Umgang im Sinne von § 202c Abs. 1 Nr. 2

[135] Dieter **Kochheim**, Skimming, 22.04.2011, S. 31.

StGB. Das Ausspähen tritt zwar in aller Regel beim Identitätsdiebstahl hinter die Computersabotage und den Computerbetrug zurück, bleibt aber wegen seiner besonderen Auswirkungen erhalten [136].

2.3.3.4 Fazit

Die einschlägige Definition von „Daten“ in § 202a Abs. 2 StGB stellt nur geringe Anforderungen an ihren personenbezogenen Gehalt und umfasst auch automatisch generierte Daten, wenn sie Auskünfte über die Person des Betreibers oder über seine interne betriebliche Organisation vermitteln (das ist eine schwache Form des Betriebsgeheimnisses, die aber schon Integritätsschutz genießt). Diese Auslegung zieht sich durch den ganzen Abschnitt über den Schutz des persönlichen Lebens- und Geheimbereichs, der die Qualität der Äußerungen ignoriert und nur danach fragt, ob das persönliche Wort mit unlauteren technischen Mitteln aufgezeichnet oder verbreitet wird (siehe zum Beispiel § 201 StGB). Auch das BVerfG setzt in seiner Entscheidung zur Onlinedurchsuchung [137] die Frage nach dem inhaltlichen Gehalt von Daten sehr flach an und nimmt aus dem Integritätsschutz nur die Datenverarbeitungen aus, die punktuell sind [138]. Es kommt deshalb im Wesentlichen darauf an, ob Daten gegen das Ausspähen durch Sicherungsmaßnahmen geschützt und ob die abgefangenen Daten für den Empfänger bestimmt sind. Soweit dabei die Infrastruktur öffentlicher Telekommunikationsdienstleister genutzt wird, ist danach zu fragen, ob das Ausspähen mit der regulären Technik der Telekommunikation erfolgt oder mit Einrichtungen, Anlagen oder Programme, die nicht für den üblichen Einsatz bestimmt sind (Abhörgeräte im Sinne von § 201 StGB). Bestimmend dafür ist, dass die TK-Dienstleister zwar Dienste für die Öffentlichkeit anbieten, die Leistung im Einzelfall aber für den Kunden und nicht für die Öffentlichkeit erfolgt. Danach sind auch öffentlich zugängliche Geräte geschützt (Webserver und andere), wenn sich das Ausspähen oder Abfangen von Daten auf die Betriebsvorgänge unterhalb des öffentlichen „Ereignishorizonts“ bezieht.

Grundsätzlich gilt der Schutz gegen Zerstörung und maßgebliche Beeinträchtigung (§§ 303a, 303b StGB) für alle handelsüblichen Haushaltscomputer und Kommunikationsgeräte, mit denen mehr als nur telefoniert werden kann, weil sie dem verfassungsrechtlichen Integritätsschutz unterliegen. In aller Regel ist die Verbreitung von Malware als Computersabotage im Sinne von § 303b StGB zu behandeln, weil bereits die Anlieferung der Malware den Tatbestand erfüllt.

Schließlich ist – neben der Ausspähung und Nutzung von Betriebsgeheimnissen (§ 17 UWG) – auch der Handel mit Zugangsdaten strafbar (§ 202c Abs. 1 Nr. 1 StGB). Somit ist zwar die Datenhehlerei als solche nicht strafbar, wohl aber drei ihrer Randbereiche: Alle Kontozugangsdaten, alle wettbewerbsrelevanten Geheimnisse und alle personenbezogenen Daten, wenn sie unlauter erschlichen wurden (§ 44 Abs. 1 in Verbindung mit § 43 Abs. 2 BDSG), nicht aber (maschinengenerierte) Daten im übrigen [139].

Als Ergebnis ist festzuhalten, dass bereits die Infiltration mit Malware und ihre Bereithaltung dazu in aller Regel als Vorbereitungshandlung und mit der

---

[136] Leitend für diesen Gedanken ist **BGH**, Beschluss vom 14.04.2011 - 1 StR 458/10; siehe auch: **CF**, Der versteckte Tatort, 03.07.2011.

[137] **BVerfG**, Urteil vom 27.02.2008 - 1 BvR 370/07, 595/07, Rn 202

[138] Auseinandersetzung mit dem ▸ Telekommunikationsrecht.

[139] Das Datenschutzrecht leidet unter systematischen Schwächen, weil es in erster Linie Verwaltungsordnungsrecht ist. Es stellt Ordnungswidrigkeiten in den Vordergrund (§ 43 BDSG) und setzt auf einige Rechtswidrigkeiten eine Strafbarkeit auf, die gleich wieder relativiert wird, weil sie einen Strafantrag voraussetzt (§ 44 Abs. 2 BDSG). Schwere Formen der gewerbs- oder bandenmäßigen Begehung werden völlig ignoriert, die Strafe ist im Bereich der leichten Kriminalität angesiedelt und Strafverfolger müssen erst um eine Ermächtigung bitten, um Handeln zu können. Mit bösen Worten: Es ist ein Strafrecht, das von vornherein nicht richtig ernst genommen werden will. Jedenfalls ist es nicht zur strategischen Strafverfolgung geeignet, allenfalls zum Beifang, und kein Ersatz für eine echte Datenhehlerei, die bei § 259 StGB angesiedelt wäre.

Zulieferung nach der Überwindung üblicher Zugangssicherungen als vollendete Computersabotage strafbar ist. Das bedeutet, dass die aktuellen Erscheinungsformen, wie Malware verbreitet wird, grundsätzlich strafbar sind und die Straffreiheit eine Ausnahme bildet.

Für eine strategische Strafverfolgung bieten zum Beispiel Pharmen und breit gestreute Spam-Mails mit Malware-Anhängen für sich alleine und ohne ihre Auswirkungen betrachtet keinen besonderen Anlass. Ihr Betrieb ist in dem Bereich der leichten Kriminalität angesiedelt und das lässt nur sehr allgemeine Ermittlungsmethoden zu. Eine Ausnahme bildet nur der Umgang mit Skimmern (Lesegeräte für Zahlungskartendaten, § 149 Abs. 1 Nr. 1 StGB), der im Bereich der mittleren und erheblichen Kriminalität angesiedelt ist (erhebliche, also gewerbs- und gewohnheitsmäßige Kriminalität im Sinne von § 110 Abs. 1 Nr. 3 StPO). Erst wenn sie ihre geplanten Wirkungen entfalten (dazu ▸ Malware in Aktion), sind sie Vorbereitungs- oder Beihilfehandlungen zu schweren Straftaten, die eine nachhaltige Strafverfolgung eröffnen.

473.480 unterschiedliche botinfizierte Computer wurden in 2010 ausfindig gemacht - jeder fünfte europäische Bot-Computer steht hierzulande. Im Durchschnitt waren pro Tag 1.946 Bots aktiv. Damit ist Deutschland der bevorzugte „Logistikstandort" für alle, die Viren, Phishing-Mails oder Spam verbreiten. Ebenso bleibt die Bundesrepublik EMEA-weit auf dem zweiten Platz nach dem Vereinigten Königreich bei Schadcodeaktivität. Zudem klettert Deutschland auf den zweiten Platz bei Phishing-Aktivitäten (2009: Platz 6) und der Verbreitung von Trojanern (2009: Platz 5).
Symantec Sicherheitsbericht: Cyberkriminalität ist deutscher Exportschlager, 05.04.2011

Deutschland sei für Cyberkriminelle ein bevorzugter Logistikstandort, wenn es um die Verbreitung von Viren, Phishing-Mails oder Spam geht. Möglicherweise ist dies auf die gute Internetinfrastruktur und die im Schnitt höhere Belastbarkeit deutscher Bankkonten zurückzuführen.
Symantec: Deutschland bevorzugter Logistikstandort für Cyberkriminelle, Heise online 05.04.2011

Versendet werden die Spam-Mails überwiegend per Botnetz. Mit einem eher kleinen Botnetz von rund 20.000 Zombie-Rechnern benötigt ein Botnetz-Betreiber für die Ausführung eines Auftrags mit 1.000.000-Mails bei beispielsweise 2 Mails pro Sekunde und aktivem Bot gerade mal 25 Sekunden. Rein rechnerisch kann ein Betreiber eines relativ kleinen Botnetzes für den Versand also bis zu 115.200 US-Dollar pro Stunde verdienen.
Sabrina **Berkenkopf**, Ralf **Benzmüller**, Gefährliche E-Mails, G Data SecurityLabs 01.06.2011, S. 3

2.4 Malware in Aktion

In diesem Abschnitt betrachten wir die Aktivitäten der Malware wegen ihres strafrechtlichen Gehalts.

2.4.1 Botware

Bereits mit der Installation von Botware wird eine Computersabotage vollendet, weil damit in aller Regel Sicherheitseinstellungen verändert, Virenscanner abgeschaltet oder manipuliert, Systemdateien verändert oder ausgetauscht, die Startkonfiguration für das Booten angepasst und schließlich zusätzliche Komponenten installiert werden (nach Bedarf: Backdoor, Fileserver, Mailserver und andere).

Der infizierte Rechner – Zombie – hat seine Integrität verloren und steht für die Fernsteuerung von außen völlig offen. Nicht nur das: Die Botware ist auf jeden Fall in der Lage, die Systemumgebung zu erkunden und dazu gehören immer die Analyse des Betriebssystems und von installierten Anwenderprogrammen sowie ihrer Versionen, die technische Leistungsfähigkeit (Festplattenspeicher, Prozessorleistung und Arbeitsspeicher) und vor allem die Zugangsdauer des Anschlusses zum Internet, die dem C&C gemeldet werden. Danach richtet sich der künftige Anwendungsbereich des Zombies. Je leistungsfähiger und „netzsicherer“ (erreichbar) er ist, desto besser lässt er sich für speicher- oder rechnerintensive Zwecke missbrauchen und das heißt als Fileserver für fremde Daten [140] (Kinderpornos, Vorpremierenfilme, ausgespähte Daten [Dumps]), als leistungsfähige Rechenmaschine [141] zum Cracking [142] oder zur Berechnung von Bitcoins [143] oder als Fluxserver [144], der anstelle des C&C-Servers im getarnten Hintergrund dessen Aufgaben für einen Teil des Botnetzes übernimmt.

Die Botwarebetreiber gehen meistens sehr behutsam mit den Zombies um. Sie sind Parasiten und sollen das Gerät in erster Linie nicht zerstören, sondern zu ihren Zwecken missbrauchen und das möglichst lange und ergiebig. Dazu gehört auch, die Botware und ihre ausführenden Aktivitäten möglichst unauffällig zu betreiben, um keine Gegenmaßnahmen zu provozieren. Der Schwund – besonders bei Flux- und Fileservern mit „riskanten“ Datensammlungen, die den C&C-Server im Hintergrund stellvertreten – ist kalkuliert und unvermeidbar.

Botnetze sind die mächtigsten Werkzeuge der Cybercrime. Ihre Einsatzmöglichkeiten und Außenwirkungen werden in den folgenden Kapiteln angesprochen. Bezogen auf den einzelnen Zombie in einem Privathaushalt drängt sich hingegen die Computersabotage durch den Betrieb von Botware nicht auf dem ersten Blick auf, zumal sie sich weitgehend unauffällig verhält. Die reine Datenveränderung (§ 303a Abs. 1 StGB) ist mit der Installation der Botware abgeschlossen, wird aber bei der Installation von Programmupdates wiederholt und vertieft. Die dauerhafte Computersabotage ergibt sich aus der Wortwahl in § 303b Abs. 1 Nr. 2 StGB, wonach die Absicht bedeutend ist, *einem anderen Nachteil zuzufügen*. Das geht über die Sachbeschädigung durch Zerstören und Unterdrücken von Dateien hinaus. Denn der ständige Nachteil besteht darin, dass der Zombie seine Integrität verloren hat, von außen gesteuert wird und der Anwender die Handlungshoheit über sein Gerät verloren hat. Selbst wenn seine Verwendungen von der Botware geduldet werden, ist der Betreiber des Botnetzes zum „Master of Desaster“ ge-

[140] Dafür eignen sich besonders die Geräte, die über große Massenspeicher (Festplatten) sowie stabile und schnelle Internetverbindungen verfügen, die im Dauerbetrieb sind. Fileserver sind insoweit einfach nur Sammelstellen für Daten, die der Angreifer zu seiner Verfügung parkt.

[141] Dabei ist nicht allein die Rechenleistung des einzelnen Zombies gefragt, sondern ihre gemeinsame Leistungskraft beim verteilten Rechnen unter dem Kommando der Botnetzsteuerung. Große Verbünde handelsüblicher PCs können die Leistung von spezialisierten Großrechenanlagen erreichen.

[142] Bekannt geworden sind bereits Botnetzeinsätze zum Knacken komplizierter Verschlüsselungen und Zugangscodes (Brute-Force-Methode).

[143] **CF**, gefährliches Spielgeld, 12.06.2011

[144] Jürgen **Schmidt**, Hydra der Moderne. Die neuen Tricks der Spammer und Phisher, Heise Security 03.09.2007

worden und kann den Anwender jederzeit von der Nutzung ausschließen.

Große Botnetze verlangen für ihren Betrieb nach etwa drei Technikern, die sich um die Aktualisierungen, Systempflege und Administration kümmern [145]. Vermutlich werden zwei weitere Vollzeit-Personen für den kaufmännischen Bereich, die Werbung und den Zahlungsverkehr benötigt. Sie wollen, das kann man bei dem betriebenen Aufwand beherzt voraussetzen, dauerhaft Geld mit dem Botnetz verdienen und handeln deswegen gewerbs- und bandenmäßig.

Nicht alle Zombies eröffnen für sich allein eine Strafverfolgung wegen einer schweren gewerbs- oder bandenmäßiger Computersabotage nach § 303b Abs. 4 Nr. 2 StGB, sondern nur die auf Geräten, *die für einen fremden Betrieb, ein fremdes Unternehmen oder eine Behörde von wesentlicher Bedeutung sind* (schwere Computersabotage, § 303b Abs. 2 StGB). Das scheidet die Geräte in reinen Privathaushalten aus, weil sie nur dem Schutz des § 303b Abs. 1 StGB unterliegen, nicht aber die PCs, die auch zur Wohnungsverwaltung, zum Nebenerwerb oder von Selbständigen zu gewerblichen Aufgaben genutzt werden (fremder Betrieb). Solche Anwender werden sich in jedem Botnetz finden lassen, vermute ich, so dass den Botnetzbetreibern Freiheitsstrafe zwischen sechs Monaten und zehn Jahren Freiheitsstrafe allein aufgrund der Tatsache droht, dass sie ein Botnetz betreiben. Dabei reicht es für die Strafbarkeit im Zusammenhang mit dem laufenden Betrieb eines Botnetzes aus, dass nur einer oder wenige der Zombies die Anforderungen der schweren Computersabotage erfüllen (§ 303b Abs. 2 StGB), weil sich dabei die Handlungen der Täter auf das Gesamtsystem und nicht allein auf den einzelnen Zombie beziehen.

Die Betrachtung des „schlichten Betriebes“ eines Botnetzes zeigt einerseits, dass der Gesetzgeber im Ergebnis mit der gewerbs- oder bandenmäßigen schweren Computersabotage eine angemessene Reaktion auf diese kriminelle Erscheinungsform gefunden hat, andererseits aber auch, dass die Rechtsfolgen von verhältnismäßig vielen Vorfragen abhängig sind, die im Zuge der Ermittlungen und schließlich in der gerichtlichen Hauptverhandlung nachvollzogen und belegt werden müssen.

Die Einrichtung und der Betrieb eines Botnetzes verlangt nach einem organisatorischen Programm, das auf geraume Zeit angelegt ist.

Von der ersten Einrichtung wird die Öffentlichkeit und die Strafverfolgung wahrscheinlich nichts oder nur wenig mitbekommen. Sie setzt die Einrichtung eines C&C-Servers voraus, der möglichst weit entfernt von agilen Strafverfolgungsbehörden im Fernen Osten oder bei Bullet-Proof-Providern in Osteuropa betrieben wird. Er stellt einige Anforderungen an die eigene Leistungsfähigkeit und an die Internetanbindung [146]. Danach muss die passende Botware mit einer Spam-Kampagne oder über präparierte Webseiten vertrieben werden.

Die nächsten Schritte zur Einrichtung des Botnetzes laufen automatisch ab. Die Malware zur Installation wird verbreitet und injiziert, worauf sich die Botware dort einnistet, wo sie für passende Exploits vorgesehen ist. Je nach Bauart meldet sie ihre Nistumgebung (Ausspähen von Daten) an den C&C und wird mit Updates, Tarnvorrichtungen gegen Virenscanner und den vom C&C bestimmten Komponenten (Backdoor, Fileserver usw) ausgestattet. Ob das ein vollständig automatischer Prozess ist oder menschliches Zutun erforderlich ist, lässt sich mit meinen Erfahrungswerten nicht hinreichend ausschließen oder untermauern. Die große Menge der schließlich eingerichteten Zombies spricht dafür, dass ihre Installation jedenfalls weitgehend automatisiert ist und nur gelegentlich menschliches Eingreifen erfordert.

---

[145] Zur Architektur von Botnetzen: **CF**, Botnet-Studie von enisa, 12.03.2011.

[146] In einem Testbetrieb in Kanada hat sich gezeigt, dass C&C-Server unter starker Last arbeiten und deshalb auf eine stark verschlüsselte Kommunikation zwischen C&C und Zombie verzichten müssen, weil sie sonst unter der Rechenlast zusammenbrechen würden.
CF, Zombies im Labortest, 21.12.2010.

Nach der Verbreitung bis zur Installation der Botware beschränkt sich die Strafbarkeit auf das Herstellen oder sich Verschaffen sowie im zugänglich machen [147] von Computerprogrammen, deren Zweck die Begehung einer solchen Tat ist (§ 202c Abs. 1 Nr. 2 StGB, Höchststrafe: Ein Jahr Freiheitsstrafe). Mangels Verbrechenstatbestände im Zusammenhang mit der Computersabotage kommt keine Beteiligung bei der Verabredung (§ 30 StGB) als strafbare Vorbereitungshandlung in Betracht.

Die Installation der Botware wird begleitet vom Ausspähen von Daten (§ 202a Abs. 1 StGB, Höchststrafe: Drei Jahre Freiheitsstrafe) und von der Zuleitung weiterer Komponenten (§ 303b Abs. 1 Nr. 2 StGB, Höchststrafe: Fünf Jahre Freiheitsstrafe, wenn es sich um eine schwere Computersabotage im Sinne von § 303b Abs. 2 StGB handelt).

Danach meldet sich die Botware beim C&C als einsatzbereit [148]. Sobald genügend Zombies zusammen gekommen sind, kann das Botnetz zum Spam-Versand oder zu anderen kriminellen Zwecken eingesetzt werden, so dass eine schwere banden- oder gewerbsmäßige Computersabotage allein wegen des Betriebes des Botnetzes angenommen werden kann (§ 303b Abs. 4 Nr. 2 StGB).

Der zwangsläufige Verlust von Zombies durch fortgeschrittene Virenscanner und Ersatzbeschaffungen muss durch Rekrutierung neuer Zombies ausgeglichen werden. Das macht weitere Verbreitungskampagnen nötig, die grundsätzlich auch den Betrieb eines Botnetzes zu einer weiteren materiellen Tat werden lassen (neu gefasster Tatentschluss). Das gilt auch dann, wenn die Täter neue Programmversionen an die laufenden Zombies verteilen. Die Einzelheiten sind noch ungeklärt.

Vieles spricht auch dafür, den Betrieb eines Botnetzes nach dem Vorbild der kriminellen Vereinigung (§ 129 StGB) als Organisationsdelikt anzusehen, so dass auf die Dauer des Betriebes bezogen nur eine materielle Tat oder einige wenige Taten zustande kommen [149]. Insoweit bleibt vor allem die Entwicklung der Rechtsprechung abzuwarten.

2.4.2 Keylogging

Vom Ursprung her sind Keylogger (unauffällige) Geräte, die an die Tastatur angeschlossen werden und alle Tastatureingaben aufzeichnen. Nach heutigem Verständnis fällt mehr darunter: Softwarelösungen und aktive Programme, die den Datenbestand gezielt nach Lizenzschlüsseln, Kontozugangsdaten und anderen personenbezogenen Daten durchsuchen, deren Nutzung oder Verkauf kriminellen Gewinn versprechen. Wenn sie den Datenverkehr überwachen, handelt es sich um ein Abfangen von Daten (§ 202b StGB), wenn sie gezielt nach ihnen suchen, um ein Ausspähen von Daten (§ 202a Abs. 1 StGB). Der Handel mit Zugangsdaten unterliegt einer selbständigen Strafbarkeit [150].

Im Zusammenhang mit Botware gibt es Hinweise darauf, dass einzelne Ausprägungen automatisch nach Lizenzschlüsseln und Zugangsdaten suchen und an den C&C übermitteln. Im laufenden Betrieb steht der Zombie jeder Manipulation durch den C&C offen und kann von dem Betreiber des Botnetzes jederzeit nach weiteren gewinnversprechenden Daten durchsucht werden.

---

147 Das semantische Problem, dass mit dem „zugänglich machen“ dem Wortzusammenhang nach nur der Verkehr mit inaktiven Computerprogrammen gemeint ist, und nicht auch mit „scharf“ gemachten Malwareprogrammen, können wir vernachlässigen: Wenn schon die „unscharfen“ Programme nicht vertrieben werden dürfen, dann gilt das umso mehr für die „scharfen“.

148 Sehr anschaulich: Kevin **Stevens**, The SpyEye Interface, Part 1: CN 1, Trendmicro 03.10.2010

149 **BGH**, Beschluss vom 19.04.2011 – 3 StR 230/10, Rn 16

150 Siehe ▸ Handel mit ausgespähten Zugangsdaten.

2.4.3 Spam

Der massenhafte Versand unerwünschter und aufgedrängter Werbenachrichten per E-Mail (Spam) ist sowohl für die Werbenden als auch für die Versender ein einträgliches Geschäft. Gehackte Server, die als Spamschleudern missbraucht werden, tauchen kaum noch auf. Das Geschäft haben die Botnetzbetreiber fast vollständig übernommen und sie werben dreist mit ihren Diensten [151]. Ihr unternehmerischer Aufwand ist unbedeutend, so dass die sonst fatale Faustformel gilt: Umsatz = Gewinn.

Das Geschäft lohnt sich aber auch für die Werbenden. Schätzungen besagen, dass nur 0,1 % der Spams erfolgreich sein müssen, um die Versandkosten wieder einzubringen [152].

Vereinzelt wird die Meinung vertreten, beim Spamming handele es sich um die Fälschung beweiserheblicher Daten (§ 269 StGB) [153], weil im Header der E-Mails regelmäßig über die Adresse des Absenders getäuscht werde. So vereinfacht ist der Argumentation nicht zu folgen, weil die Besonderheiten der Urkundenfälschung berücksichtigt werden müssen, in deren Abschnitt der § 269 StGB angesiedelt ist. Zur Verdeutlichung muss zunächst auf das Wesen von Urkunden und auf die Schwierigkeiten eingegangen werden, die die Rechtsprechung bereits bei ihrer Bewertung von Faxen und computerbearbeiteten Bildern hat.

2.4.3.1 Urkunde und Abbild

Urkunden im Sinne des Strafrechts sind verkörperte Erklärungen, die ihrem gedanklichen Inhalt nach geeignet und bestimmt sind, für ein Rechtsverhältnis Beweis zu erbringen, und die ihren Aussteller erkennen lassen [154].

Damit sind drei bestimmende Voraussetzungen erforderlich: Die Urkunde muss die Verkörperung einer Gedankenerklärung eines bestimmten Ausstellers sein, die im Rechtsverkehr eine gestaltende Wirkung hat. Daran fehlt es zum Beispiel bei der schriftlichen Lüge, wenn der Aussteller zwar nicht über seine Identität täuscht, aber einfach nur eine Unwahrheit erklärt. Das mag ein Täuschungsmittel zur Begehung eines Betruges sein (§ 263 StGB), aber keine Urkundenfälschung (§ 267 StGB).

Fotokopie und Telefax sind *nur die bildliche Wiedergabe der* <im Original> *verkörperten Erklärung* [155], ohne dass sie als offensichtliches Abbild selber zur Urkunde werden. Nur ausnahmsweise dann, wenn die Kopie ***als*** ein Original verwendet wird, kann es sich um den Gebrauch einer falschen Urkunde handeln, wenn sich aus dem Abbild auf der Kopie kein Hinweis darauf ergibt, dass es sich um eine Wiedergabe handelt [156]. Das gilt auch für computerbearbeitete Kollagen: Die Einbindung von Unterschrifts-Paraphen angeblicher Vertragspartner machen die optisch verfälschte Computerdatei nicht zur *Urkunde, da das Schriftstück nach außen als Reproduktion erscheint* [157]. *Zwar kann im Wege computertechnischer Maßnahmen wie der Veränderung eingescannter Dokumente grundsätzlich eine (unechte) Urkunde hergestellt werden. Dafür muss die Reproduktion jedoch einer Originalurkunde so ähnlich sein, dass die Möglichkeit einer Verwechslung nicht ausge-*

---

[151] Sabrina **Berkenkopf**, Ralf **Benzmüller**, Gefährliche E-Mails, G Data SecurityLabs 01.06.2011

[152] Alfred Krüger, Angriffe aus dem Netz. Die neue Szene des digitalen Verbrechens, Heise Verlag 2006, S. 66

[153] a-i3/BSI Symposium 2006, Phishing und Online-Banking, 2006

[154] **BGH**, Beschluss vom 23.03.2011 – 5 StR 7/10, Rn 4

[155] **BGH**, Beschluss vom 27.01.2010 - 5 StR 488/09, Rn 10; so auch schon: **BGH**, Urteil vom 11.05.1971 - 1 StR 387/70.

[156] **BGH**, Urteil vom 14.09.1993 - 5 StR 283/93

[157] **BGH**, Beschluss vom 23.03.2011 – 5 StR 7/10, Rn 4 am Ende

schlossen werden kann [158]. *Da der von den Ausdrucken der Computerdatei jeweils abgebildete Personalausweis tatsächlich nicht existierte und diesbezüglich somit zu keinem Zeitpunkt eine falsche Urkunde vorgelegen hat, erfüllt die Verwendung dieser Ausdrucke auch nicht den Tatbestand der Urkundenfälschung in Form des Gebrauchens einer unechten Urkunde* [159].

Beglaubigungsvermerke auf einer Kopie sind hingegen *eine Urkunde, so dass eine unechte Urkunde hergestellt wird, wenn ein Beglaubigungsvermerk gefälscht wird* [160], nicht aber der Absenderaufdruck auf einem Fax [161].

Daraus folgt, dass jede Reproduktion, die nicht den Anspruch erhebt, selber das Original zu sein, keine Urkunde im Sinne von § 267 StGB ist. Die beschriebenen Grundsätze sind auch auf beweiserhebliche Daten im Sinne von § 269 StGB anzuwenden [162].

So hat der BGH unlängst entschieden[163]: *Durch die Ausdrucke von Bilddateien eines Personalausweises unter manipulativer Änderung von Personaldaten und Lichtbild sind weder unechte oder verfälschte Urkunden hergestellt worden, noch hat der Angeklagte solche Urkunden gebraucht, indem er die Ausdrucke verwendete, um vorzutäuschen, dass von den fiktiven Kunden Personaldokumente vorgelegen hätten. ... Da der von den Ausdrucken der Computerdatei jeweils abgebildete Personalausweis tatsächlich nicht existierte und ... somit zu keinem Zeitpunkt eine falsche Urkunde vorgelegen hat, erfüllt die Verwendung dieser Ausdrucke auch nicht den Tatbestand der Urkundenfälschung in Form des Gebrauchens einer unechten Urkunde.*

2.4.3.2 E-Mail als Urkunde

Die Received-Einträge im Header einer E-Mail geben ihren Weg wieder, den sie im Internet durchlaufen hat. Der unterste Eintrag ist für den absendenden Mailserver reserviert und kann vom Versender manipuliert werden. Das gilt auch für die weiteren Stationen, wenn der Versender auf sie einen unmittelbaren Zugriff hat. Sobald jedoch die Adressen der üblichen Carrier oder Netzknoten als „Received“ erscheinen, ist eine Manipulation unwahrscheinlich oder sogar der Erfahrung nach ausgeschlossen.

Zu Recht stellt die Kommentarliteratur eine digitale Fälschung im Zusammenhang mit der Internetadresse des Absenders in Frage, weil sie weder aussagestark für die Identität noch für die Gedankenerklärung des (angeblichen) Ausstellers ist [164]. Sie ist so zu behandeln wie der Absenderaufdruck beim Fax. Insoweit kann sie zwar ein Indiz für die Authentizität der Nachricht, also ein Beweisanzeichen, nicht aber eine Urkunde mit eigenem Aussagewert sein.

Das sieht bei nachgemachten Webseiten (Pharming) anders aus. Kommerzielle Webseiten werden regelmäßig von privaten Unternehmen zertifiziert. Dabei handelt es sich um eine verschlüsselte Signatur, die von einer Zertifizierungsstelle mit ihrem Zertifikat signiert ist [165]. Der Browser des Anwenders prüft das Zertifikat gegen seine interne "trust list" und lässt erst bei einer Übereinstimmung eine sichere Verbindung nach dem Protokoll für Secure Sockets Layer – SSL – zu [166]. Dabei handelt es sich in der Tat um einen Datenverarbeitungsvorgang (§ 270 StGB), bei dem jedenfalls dem Zertifikat ein urkundlicher Beweischarakter im Sinne von § 269 Abs. 1 StGB zukommt. Gefälschte Zertifikate sind bereits im Laborversuch herge-

---

158 **BGH**, Beschluss vom 09.03.2011 - 2 StR 428/10, Rn 3

159 Ebenda

160 **BGH**, Urteil vom 14.09.1993 - 5 StR 283/93

161 **BGH**, Beschluss vom 27.01.2010 - 5 StR 488/09, Rn 11

162 **BGH**, Beschluss vom 27.01.2010 - 5 StR 488/09, Rn 13

163 **BGH**, Beschluss vom 09.03.2011 - 2 StR 428/10, Rn 9, 11; siehe auch **CF**, PhotoShop und Urkunde, 15.06.2011.

164 Fischer, § 269 StGB, Rn 8

165 **CF**, Kollisionsangriff gegen Webseitenzertifikat, 15.02.2009

166 Transport Layer Security - TLS

stellt [167] und echte massenhaft gestohlen worden [168]. Dasselbe Ergebnis würde auf E-Mails zutreffen, die fortgeschritten oder qualifiziert signiert sind und deren Signatur gefälscht ist [169]. Dafür gibt es aber noch keine Beispiele.

Anders ist die offene Gestaltung einer E-Mail oder einer nachgemachten Webseite zu behandeln. Dabei kann der Versender durch seine Wortwahl, durch das Layout und die Einbindung (häufig sogar der Originalbilder) von Grafiken den Anschein erwecken, sie stamme von einem bestimmten und existierenden Aussteller, einer Bank, Handelsunternehmen oder Behörde, so dass tatsächlich § 269 StGB greift. Das gilt nicht, wenn Phantasienamen verwendet - „Volksbank AG“ - oder zauberhafte Geschichten in der Tradition der Nigeria Connection erzählt werden [170].

Bei der Verwendung fremder Namen, Marken, Embleme und Gestaltungselemente können auch gewerbliche Schutzrechte betroffen sein. Das gilt zunächst wegen der Vervielfältigung urheberrechtlich geschützter Werke und beim unzulässigen Anbringen einer Urheberbezeichnung. Der Urheberschutz (§ 106 Abs. 1 UrhG) gilt auch für aufwändige Grafiken und künstlerische Fotos, die in Spam-Mails oder nachgemachte Webseiten eingebunden werden. Nachgemachte Grafiken, Texte und Kompositionen, denen eine falsche Urheberbezeichnung zugefügt werden, unterliegen ebenfalls der Strafbarkeit (§ 107 Abs. 1 Nr.1 UrhG) – in beiden Fällen mit bis zu drei Jahren Freiheitsstrafe. Dasselbe gilt für die unerlaubte Verwendung von Markennamen und -symbolen (§ 143 Abs. 1 MarkenG) [171].

[167] Siehe: **CF**, Kollisionsangriff ...

[168] **CF**, RSA-Hack, 07.04.2011

[169] Elektronische Signatur

[170] Siehe: Sabrina **Berkenkopf**, Ralf **Benzmüller**, Gefährliche E-Mails, G Data Whitepaper 6/2011, 01.06.2011, S. 13

[171] Eine sprachliche deutsche ~~Kuriosität~~ Besonderheit stellt das Geschmacksmustergesetz dar. Es betrifft nicht etwa den sinnlichen Geschmack, sondern die Präsentation und Beschaffenheit von Handelsprodukten.

2.4.3.3 Fazit

Die Verbreitung von Spam-Mails ist nicht immer strafbar. Falsche Adressangaben für den Absender sind jedenfalls keine digitale Urkunden, die von § 269 StGB geschützt werden würden, sondern als Indiztatsachen wie die Absenderzeile beim Fax zu behandeln, der auch keine eigenständige Urkundsbedeutung zukommt.

Wenn aber die Gestaltungselemente von Firmen, Banken oder Behörden verwendet werden, um einer Spam-Mail einen offiziellen Anstrich zu geben, dann greift der Urkundenschutz des § 269 StGB. Durch den Verweis in § 269 Abs. 3 StGB auf § 267 Abs. 3 und 4 StGB werden die besonders schweren Fälle zu Vergehen mit zehn Jahren Höchstfreiheitsstrafe und die gewerbs- und bandenmäßige Begehung zu einem eigenständigen Verbrechen, das mit Freiheitsstrafe von einem bis zu zehn Jahren Freiheitsstrafe droht.

Diese Folgen betreffen die Betreiber von Botnetzen, von Pharmen und Onlinebanking-Trojanern besonders stark.

Professionelle Botnetzbetreiber planen – dafür sprechen die Erfahrungen – von vornherein, Spam-Mails ungeachtet ihrer urkundlichen Qualität zu verbreiten. Dazu gehört die Werbung für illegale Medikamente (Viagra, Penisverlängerungen usw), Fakes in allen Formen, also auch von nachgemachten Banknachrichten, die Zuschriften anderer gewerblicher Handelsplattformen und die Sauereien, die heute im Zusammenhang mit der Cybercrime üblich sind. Dadurch werden die Betreiber vermieteter Botnetze grundsätzlich zu tatvorbereitenden Mittätern der Ausführungstäter, die zum Beispiel das Fälschen beweiserheblicher Daten im Zusammenhang mit dem Onlinebanking-Betrug betreiben (oder anderer Formen des Identitätsdiebstahls), wofür es im Wiederholungsfall (Tatmehrheit, § 53 StGB) bis zu 15 Jahren Freiheitsstrafe geben kann (§§ 38 Abs. 2, 54 Abs. 2 S. 2 StGB).

2.4.4 Malware-Versand

Die häufigste Methode, Malware zu verbreiten, bedient sich der Spam-Nachrichten. Drei wesentliche Methoden für die Infektion können dabei unterschieden werden.

Die Nachricht kann über einen Anhang verfügen, der sich als Datei für ein bestimmtes Programm ausgibt (Textdatei, Präsentation, PDF). Tatsächlich handelt es sich aber um einen Trojaner, in dem die Malware eingebunden ist [172]. Beim Start der Datei wird die Programmumgebung des Anwenderprogramms gestartet und diese gibt damit auch der Malware die Umgebung, um sich einzunisten. Dieser Vorgang erfolgt automatisch, so dass sich das Täterhandeln auf den bewussten Start der Spam-Aktion beschränkt.

Bei strenger wörtlicher Betrachtung ist die „Übermittlung“ im Sinne von § 303b Abs. 1 Nr. 2 StGB bereits abgeschlossen, sobald der Dateianhang dem Mail-Browser zum Start präsentiert wird. Das wird den übrigen Tatbeständen der Computersabotage aber nicht gerecht, die auf den zerstörerischen Erfolg abstellen. Deshalb muss wohl davon ausgegangen werden, dass die Übermittlung erst beendet ist, wenn die Malware an einen ***aktiven Prozess*** abgegeben wird, unter dem sie sich selbständig ausführen kann und das wäre erst beim Start des Anwenderprogrammes anzunehmen, mit dem zusammen die Malware ausgeführt werden soll.

Diese Lösung vermeidet ein weiteres, praktisches Problem. Je nach den Einstellungen des Browsers und seiner Bauart werden Dateianhänge auf dem lokalen Gerät häufig nur angezeigt und erst übermittelt, sobald sie vom Anwender gestartet werden. Dabei fallen der Dateistart und der letzte Schritt der Übermittlung von Malware in einem vom Anwender gesteuerten Handlungsakt zusammen. Sähe man die Übermittlung im Sinne von § 303b Abs. 1 Nr. 2 StGB bereits mit der Anlieferung zum Browser als vollendet an, dann müsste man in jedem Fall rückwirkend die Browsereinstellungen erheben und nach den beiden Übermittlungsmethoden im Einzelfall unterscheiden. Bei der hier vorgeschlagenen Auslegung tritt die Vollendung erst mit der Zulieferung der Malware an einen aktiven Prozess ein. Alle davor liegenden Zulieferungsschritte, die mit dem Start der Spam-Kampagne durch den Täter als letzte persönliche Handlung begann, sind noch im strafbaren Versuchsstadium angesiedelt (§ 303b Abs. 3 StGB).

Eine andere Injektionsmethode greift Schwachstellen im Browser selber an. Bei ihr ist der Starter für die Malware entweder im Textkörper der Nachricht oder in dynamischen Elementen eingebunden, die für die Anzeige der Nachricht zugeliefert werden. Ein bekanntes Beispiel für Manipulationen mit dem Textkörper liefern die ▸ iFrames, mit denen unbemerkt schädlicher Code geladen werden kann. Er besteht meistens nur in einem verhältnismäßig kurzen Startkommando, das den Browser zum selbsttätigen Laden der Malware veranlasst. Der hier vertretenen Auffassung folgend, ist die Übermittlung abgeschlossen, sobald der Browser den Starter ausführt. Dasselbe gilt für Starter, die in Grafiken oder anderen dynamischen Elementen eingebunden sind (Sounds, Animationen) und für präparierte Webseiten.

Die dritte wichtige Methode zur Injektion von Malware wird mit Hyperlinks ausgeführt, die im Text der Nachricht unterlegt sind. Das häufig verwendete HTML-Format lässt es im Interesse der Lesbarkeit zu, dass auf der Oberfläche ein anderer Text angezeigt wird als die Adresse, auf die der Link zeigt [173]. Mit diesen Links soll der Anwender zu präparierten Webseiten geführt werden, wo er entweder zu unbedachten Dateneingaben veranlasst werden soll oder die mit Injektionsmechanismen ausgestattet sind, die der beschriebenen Art entsprechen.

---

[172] Schon 2008 wurde von Trojaner-Baukästen mit einer eingängigen Windows-Oberfläche berichtet, mit der die Angriffseigenschaften einfach „zusammengeklickt“ werden: F-Secure, Creating Malicous PDF Files, 02.06.2008; Angriffe über präparierte PDF-Dateien werden ausgefeilter, Heise online 03.06.2008.

[173] Einzelheiten: Dieter **Kochheim**, Cybercrime, 24.06.2010, S. 24 (Nummerntricks. Adressenschwindel bei Telefondiensten und im Internet).

In diesem Fall ist die Strafbarkeit ganz anders zu bewerten. Mit der Präsentation präparierter Links wird in die Datenverarbeitung des Anwenders noch nicht eingegriffen. Die Schadfunktion steckt, anders als beim Starterkommando, nicht im Link selber, sondern erst in der präparierten Webseite, zu der der Anwender geführt werden soll. Die Verbreitung dieser Links ist also vollständig im Vorbereitungsstadium angesiedelt. Eine Strafbarkeit im Vorbereitungsstadium sieht § 303b Abs. 5 StGB unter Bezugnahme auf § 202c StGB aber nur im Hinblick auf die Verbreitung oder das Zugänglichmachen von Passwörtern, Sicherungscodes und Computerprogrammen zum Abfangen oder Ausspähen von Daten vor. Diese Tatbestände passen alle nicht auf die Zulieferung von Links, mit denen der Anwender erst auf präparierte Seiten gelockt werden soll.

Wegen der Strafbarkeit von Spam-Nachrichten, die zur Verbreitung von Malware bestimmt sind, ist deshalb danach zu unterscheiden, ob sie die schädliche Funktion in sich selber tragen (Trojaner als Anhänge, Starterkommandos) oder ob sie nur über Links zu präparierten Webseiten verfügen. In diesem Fall handelt es sich um eine noch straflose Vorbereitungshandlung. In den beiden ersten Fällen wird hingegen mit der Übermittlung der Malware an ein aktives Anwenderprogramm die Computersabotage gemäß § 303b Abs. 1 Nr. 2 StGB vollendet.

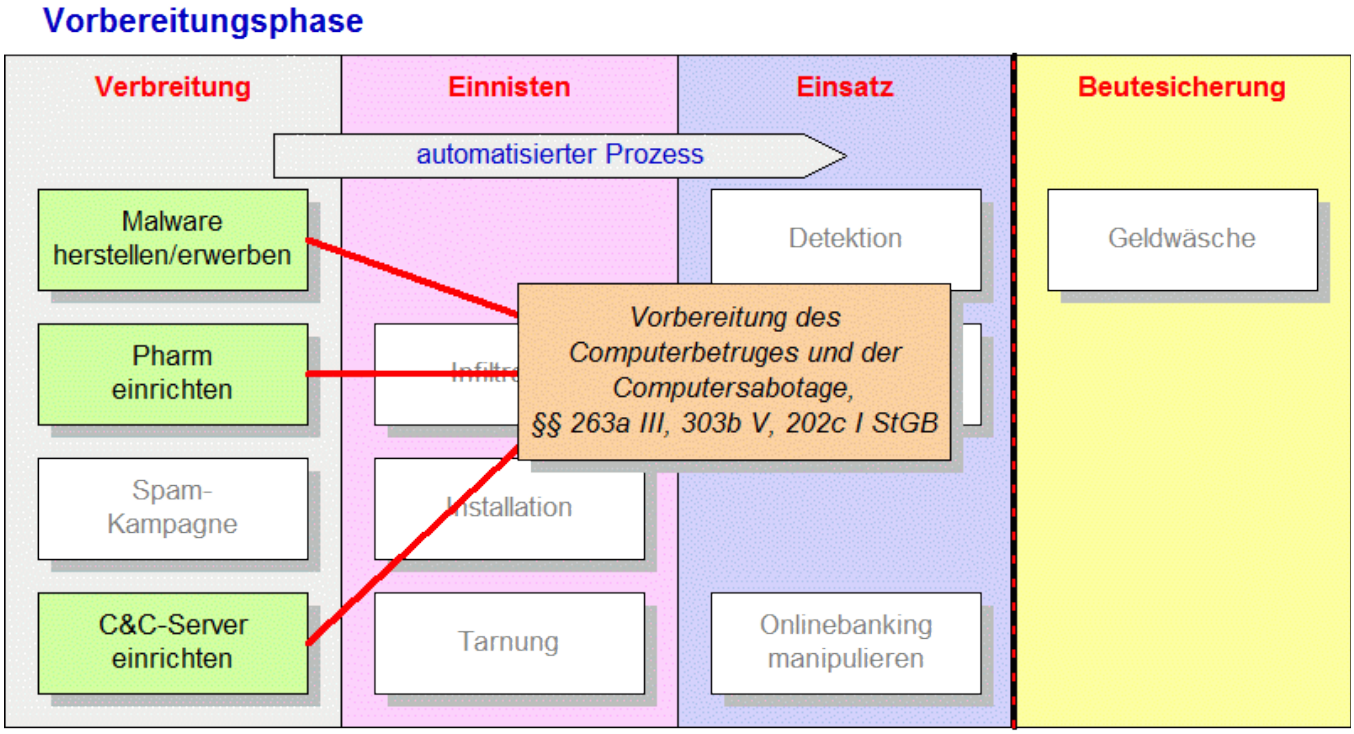
Wegen der präparierten Webseiten muss schließlich geprüft werden, welche schädlichen Aktivitäten sie tatsächlich ausführen. Beschränken sie sich darauf, den Anwender zu unbedachten Dateneingaben zu veranlassen, kommt allenfalls eine Strafbarkeit nach § 202c Abs. 1 Nr. 1 StGB in Betracht (Verschaffen von Passwörtern oder sonstige Sicherungscodes), weil nur der Vorgang der Dateneingabe überwacht wird [174] und kein Ausspähen oder Abfangen von Daten vorliegt (§§ 202a Abs. 1, 202b StGB).

[174] Dieses Problem stellt sich auch bei dem Ausspähen der PIN beim Skimming. Es handelt sich um ein Ausspähen bei der Dateneingabe, die vom Datenbegriff in § 202a Abs. 2 StGB nicht erfasst ist. Siehe: Dieter **Kochheim**, Skimming, 22.04.2011, S. 20 (Abfangen von Daten).

Schema: Einsatz eines Homebanking-Trojaners

	Anwender	Malware	C&C	Bank
1.1	A ruft die Webseite seiner Bank auf	▸	▸	
1.2		MW protokolliert Aufruf und Daten		
1.3		◂	◂	B meldet Zugangsprozedur
1.4	A gibt Kontodaten und Captcha ein	▸	▸	
1.5		MW meldet Kontozugang und die protokollierten Daten		
1.6		◁ MW kappt die Verbindung und leitet auf C&C um	↪	B meldet Übersichtsseite
2.1		MW vermittelt die Kommunikation zwischen Anwender, C&C und Bank	C&C liefert über die MW Daten für eine Überweisung	
2.2			C&C generiert Bankseite (Sicherheitshinweis) und fordert iTAN an	B fordert iTAN an
		◂	◂	
2.3	A gibt iTAN ein	MW gibt iTAN weiter		
			▸	
2.4			C&C generiert eigene Bankseite ohne Überweisungsdaten	B bestätigt Überweisung
		◂	◂	
3.1	A startet eigene Überweisung	➤	C&C generiert über die MW eine weitere Überweisung	
3.2			C&C generiert mit den Daten von A Bankseite und fordert iTAN an	B fordert iTAN an
		◂	◂	
3.3	A gibt iTAN ein	MW gibt iTAN weiter		
			▸	
3.4			C&C bestätigt mit den Daten von A die Überweisung	B bestätigt Überweisung
		◂	◂	
4.1	A beendet die Session	MW gibt Logout weiter und meldet sich beim C&C ab	▸	
4.2		MW kappt die Verbindung und verhindert den Neustart für das Internet		

Oben: Zusammenspiel eines Onlinebanking-Trojaners mit einem Command and Control Server – C&C – bei der Manipulation einer Session zwischen Anwender und Bank (Erläuterung im folgenden Text).



Bereits die ersten Tathandlungen sind für sich einzeln betrachtet als selbständige Vorbereitungstaten strafbar.

Nur die Verbreitung schlichter Spam-Mails ohne urheber- oder markenrechtliche Besonderheiten ist strafrechtlich bedeutungslos, wenn sie keine Malwarefunktionen in sich selber tragen (Links zu präparierten Seiten, HTML-Funktionen, Trojaner-Anhänge).

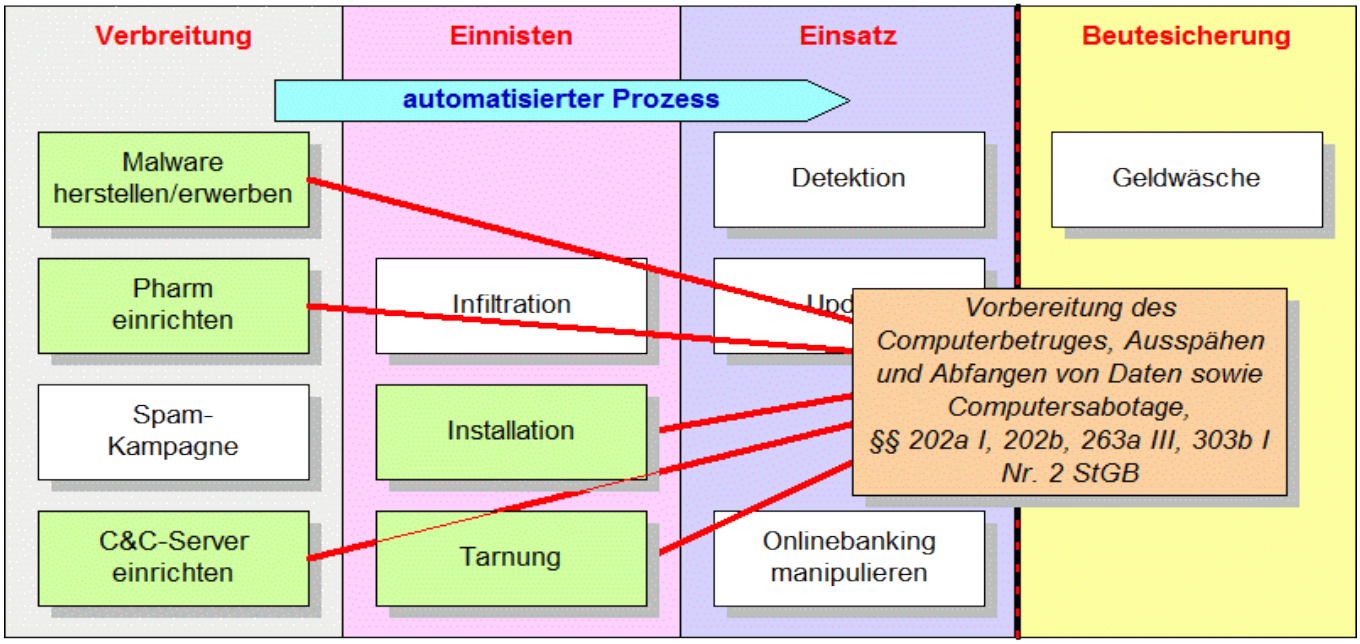
2.4.5 Onlinebanking

Als moderne Form des ▸ Phishings wurde ein vollautomatischer Trojaner vorgestellt, der im Zusammenspiel mit einem Command and Control-Server – C&C – den kompletten Vorgang des Homebankings überwacht und schließlich zur Manipulation missbraucht. Der geschilderte Vorgang ist nicht nur tatsächlich, sondern auch rechtlich kompliziert. Das Schaubild auf der ▸ vorigen Seite soll beim Verständnis helfen.

Während der Anwender die Webseite für das Onlinebanking aufruft und die Zugangsdaten samt Captcha eingibt <1.1 bis 1.4>, protokolliert die Malware nur den Zugang zum Onlinebankingkonto (Abfangen von Daten, § 202b StGB; diese Tat dauert während der ganzen Session an). Sobald die Bank ihre Übersichtsseite meldet, unterdrückt die Malware deren Ausgabe auf den Bildschirm <1.5, 1.6> (Urkundenunterdrückung, § 274 Abs. 1 Nr. 2 StGB) und fordert vom C&C Anweisungen an. Für alle weiteren Vorgänge wird die Malware zur Vermittlungsstelle zwischen Bank, Anwender und C&C.

Vom C&C erhält die Malware Daten, um damit eine Überweisung zu generieren <2.1>, die die Malware an die Bank weiterleitet (versuchte Fälschung beweiserheblicher Daten und versuchter Computerbetrug, § 269 Abs. 1, Abs. 2, § 263a Abs. 1, Abs. 2 StGB). Darauf fordert die Bank eine bestimmte iTAN an <2.2>. Diese Meldung fängt die Malware ab (Urkundenunterdrückung, § 274 Abs. 1 Nr. 2 StGB) und fordert vom C&C eine neue Bankseite an, die dem Anwender zum Beispiel neue Sicherheitsmaßnahmen ankündigt, die er durch die Eingabe der von der Bank angeforderten iTAN aktivieren muss (Fälschung beweiserheblicher Daten, § 269 Abs. 1 StGB). Sobald der Anwender die geforderte iTAN eingegeben hat <2.3> (Betrug, § 263 Abs. 1 StGB) leitet die Malware die iTAN an die Bank weiter. Die Bestätigung der Bank über die Verfügung (Computerbetrug, § 263a Abs. 1 StGB) wird wiederum von der Malware abgefangen <2.4> (Urkundenunterdrückung, § 274 Abs. 1 Nr. 2 StGB) und sie fordert wiederum

Installation



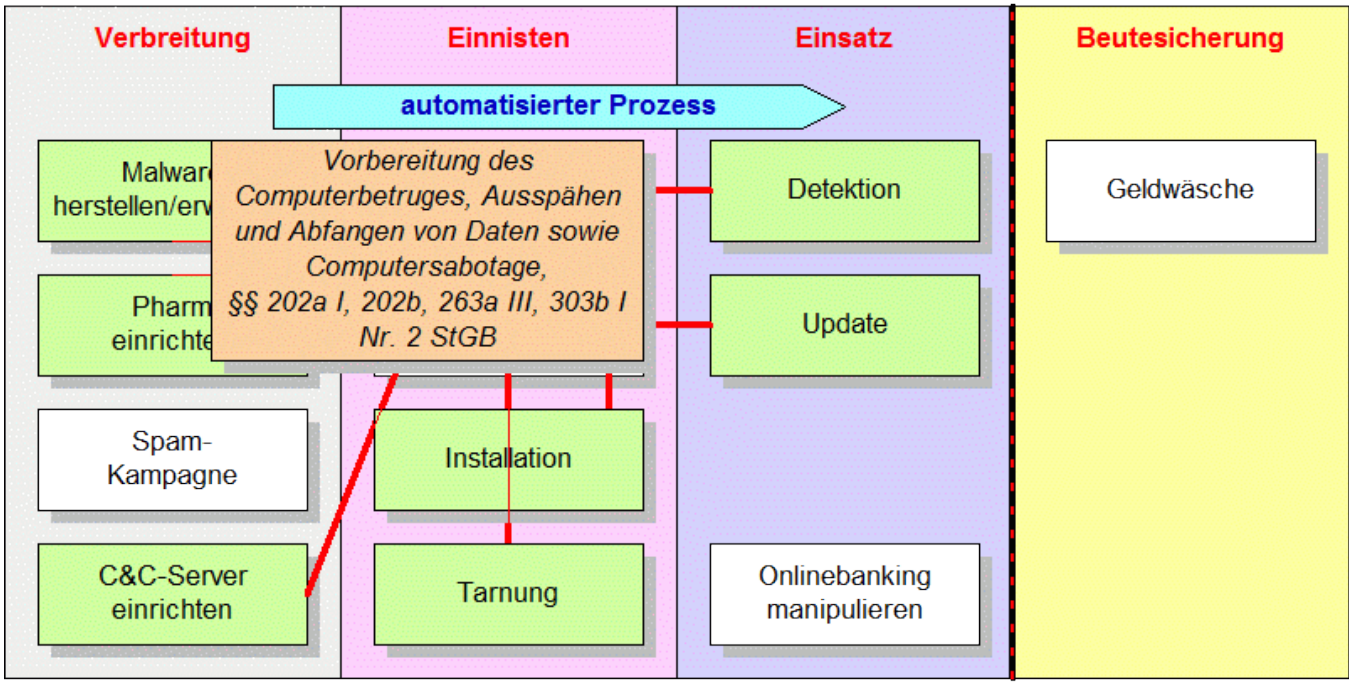
Anschließend startet ein automatisierter Prozess, in dessen Verlauf sich die kriminellen Folgen verändern und verschärfen, ohne dass die Täter einen aktiven Anteil daran haben. Sie haben ihn jedoch angestoßen und mit Vorsatz gewollt, so dass der Erfolg ihnen auch strafrechtlich zuzurechnen ist.

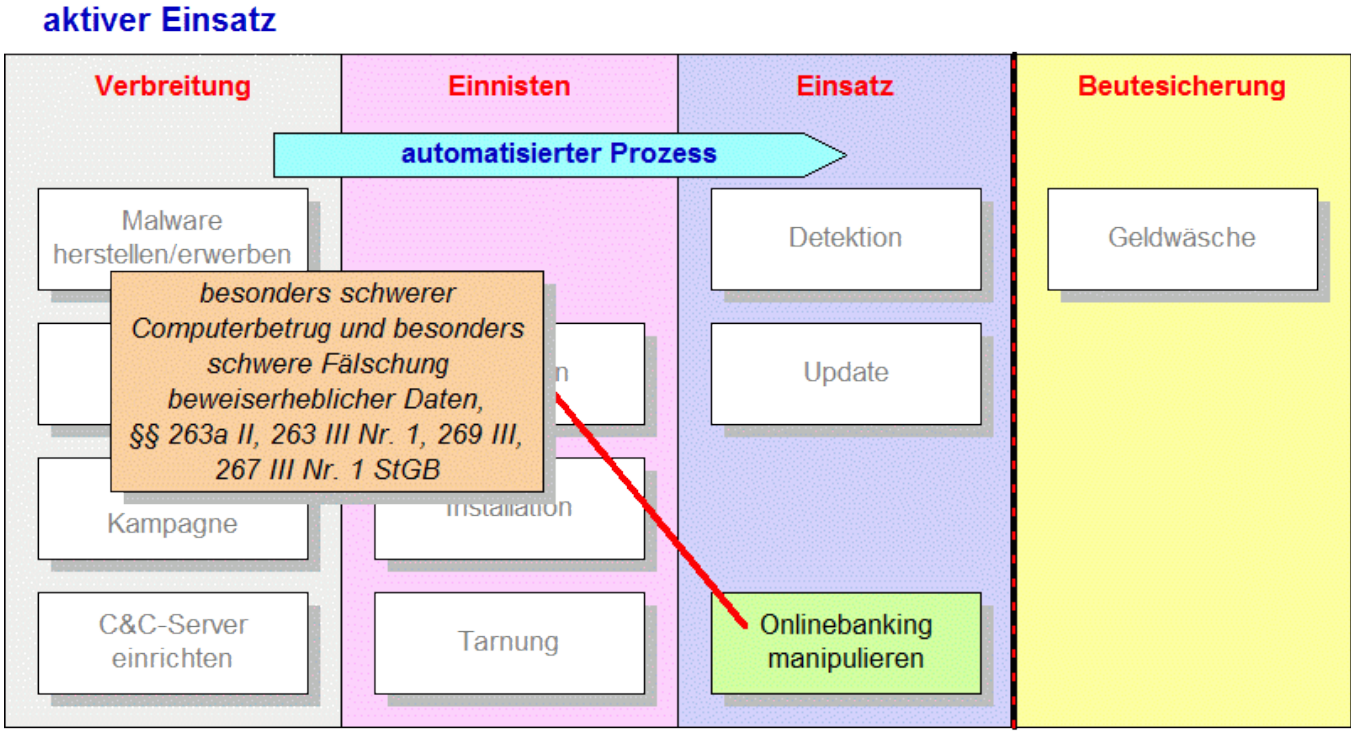
Nur die Infiltration der Malware basiert jedenfalls dann, wenn sie über den Browser erfolgt, auf öffentlichen Meldungen, die die Malware aufnehmen kann, ohne dass sie nicht für sie bestimmte oder gegen das Ausspähen geschützte Daten verarbeitet. Alle anderen Prozessschritte verschärfen nach und nach die kriminelle Schwere des Angriffs.

Während des „schlafenden“ Einsatzes hält sich die Malware zurück und detektiert nur die Umgebungsaktivitäten. Dabei nimmt sie regelmäßig Kontakt zum C&C auf, um neue Anweisungen oder Updates zu erhalten. Bei Updates wird der Vorgang wiederholt, der auch bei der Installation durchgeführt wurde.

Bei der Frage nach der materiellen Tatmehrheit muss darauf geachtet werden, ob sich im Update ein neuer Tatentschluss äußert. Das dürfte der Fall sein, wenn ein ganzes System betroffen ist (Botnetz, viele Onlinebanking-Trojaner), nicht aber bei einem einzelnen Trojaner.

"schlafender" Einsatz





Sobald der Anwender mit dem Homebanking beginnt, löst die Malware den finalen Prozess aus, der mit der Fälschung beweiserheblicher Daten einher geht und zum Computerbetrugsschaden führt.

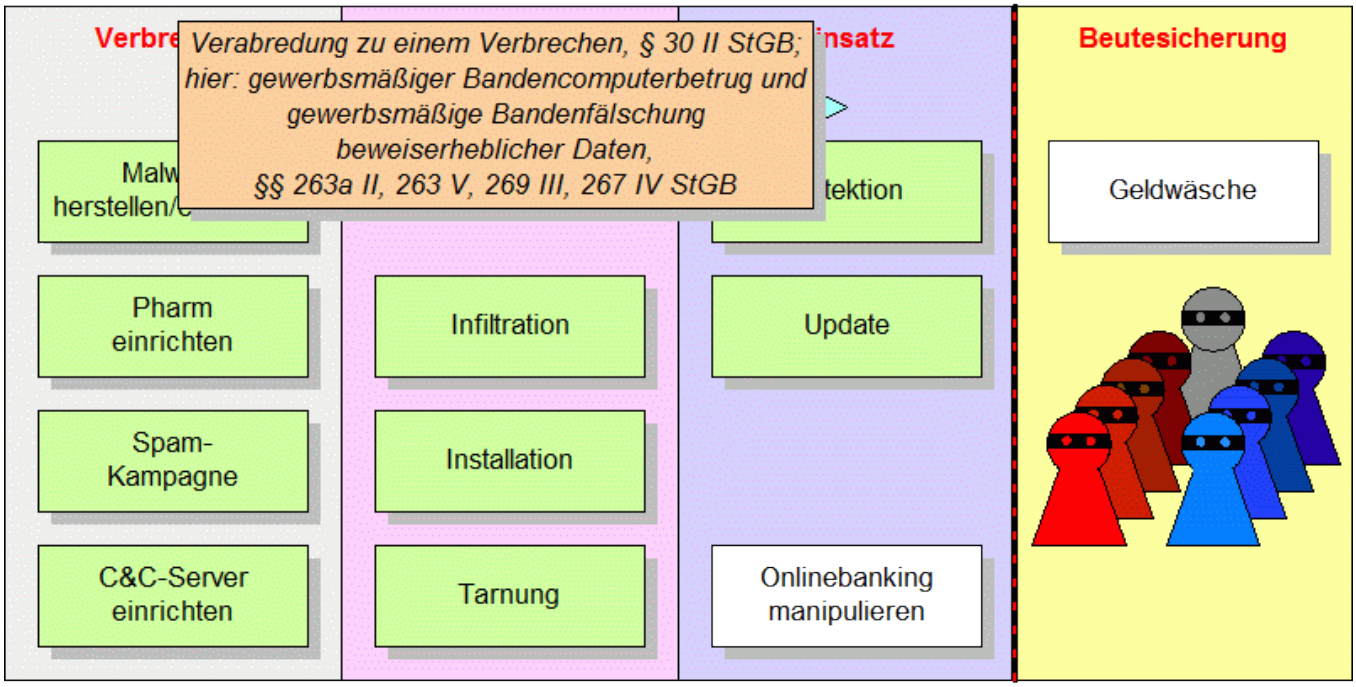
Das löst eine ganze Folge von Tatbestandsverstößen aus, wobei von ihrer Schwere her maßgeblich die besonders schweren Fälle des Computerbetruges und der Fälschung beweiserheblicher Daten sind, wenn man gewerbsmäßiges Handeln voraussetzt. Der betriebene Aufwand lässt grundsätzlich keinen anderen vernünftigen Schluss zu.

vom C&C eine Bankseite ab, die die ausgeführte Überweisung nicht erkennen lässt. Diese sendet die Malware an den Anwender (Fälschung beweiserheblicher Daten, § 269 Abs. 1 StGB). Im ▸ Schaubild wird noch eine weitere Überweisung durchgeführt, die dem gleichen Schema folgt <3.1 bis 3.4>. Am Ende meldet sich der Anwender bei der Bank ab, was die Malware brav weiter gibt. Das nimmt die Malware zum Anlass, die interne Konfiguration des PCs des Anwenders abzuändern, damit er zunächst nicht mehr ins Internet gelangen und womöglich die Überweisungen stornieren kann (Computersabotage, § 303b Abs. 1 Nr. 1 StGB).Die Konkurrenzverhältnisse zwischen den betroffenen Strafvorschriften sind komplex, so dass es sich auch an dieser Stelle lohnt, nach dem leitenden Täterwillen zu fragen. Der ist darauf ausgerichtet, am Ende Beute zu machen, und die filigranen Zwischenschritte sind notwendige Akte, um das finale Ziel zu erreichen. Im Vordergrund steht also ein Computerbetrug gemäß § 263a Abs. 1 StGB (unbefugte Verwendung von Daten), der im Grundtatbestand mit Freiheitsstrafe bis zu fünf Jahren droht.

Der Schritt <2.3> erfordert eine bewusste Preisgabe der iTAN vom Anwender, der in dem Irrtum ist, die iTAN werde dafür gefordert, neue Sicherheitsmechanismen zu aktivieren. Die vom C&C dazu generierte Seite ist ausdrücklich auf die Täuschung eines Menschen ausgerichtet und nicht auf die Manipulation eines Datenverarbeitungsvorganges beim Computerbetrug. Betrug und Computerbetrug schließen sich hingegen tatbestandlich aus [175], so dass der tatbeherrschende Tatbestand des Computerbetruges in den Vordergrund tritt. Die betroffenen Tatbestände im übrigen – Ausspähen von Daten (§ 202a Abs. 1 StGB), Abfangen von Daten (§ 202b StGB), Datenverände-

[175] Fischer, § 263a StGB, Rn 39

Verabredung zu einem Verbrechen (Bande)



Handeln die Täter als Bande, wandelt sich die Beurteilung komplett. Ihre Tatplanung soll zu einem tateinheitlichen Verbrechen des gewerbsmäßigen Bandencomputerbetruges und der gewerbsmäßigen Bandenfälschung beweiserheblicher Daten führen.

Dadurch werden ihre Vorbereitungshandlungen zu Teilakten des geplanten Verbrechens, ohne dass es einer finalen Tatbestandsmerkmalverwirklichung bedarf. Alle Ausführungshandlungen bestätigen die getroffene Anbrede, wenn sie als solche nachweisbar ist.

rung (§ 303a StGB) und Computersabotage (§ 303b Abs. 1 StGB) sowie die Fälschung (§ 269 Abs. 1 StGB) und Unterdrückung beweiserheblicher Daten (§ 274 Abs. 1 Nr. 2 StGB) können grundsätzlich eine Tateinheit (§ 52 StGB) bilden [176], wobei das Gesetz mit der schwersten Strafdrohung Ausschlag gebend ist. Insoweit sind die Tatbestände der §§ 263a, 269 und 274 Abs. 1 Nr. 2 StGB gleichwertig.

Die Computersabotage ist eine erweiterte und qualifizierte Form der Datenveränderung, so dass § 303a StGB verdrängt wird. Dem Ausspähen von Daten kommt beim automatisierten Phishing eine völlig nachgeordnete Rolle zu, so dass auch § 202a Abs. 1 StGB von den Tatbeständen im übrigen verdrängt wird.

Dies vorausgesetzt haben wir es beim Einsatz eines völlig automatisierten Onlinebanking-Trojaners mit einem Computerbetrug in Tateinheit mit Abfangen von Daten, Computersabotage sowie der Fälschung und Unterdrückung beweiserheblicher Daten gemäß §§ 263a Abs. 1, 202b, 303b Abs. 1, 269 Abs. 1 und 274 Abs. 1 Nr. 2 StGB zu tun.

Ich bin davon überzeugt, dass die hoch entwickelten Formen der Malware im Zusammenhang mit Botnetzen und dem Homebanking im Betrieb automatisiert sind und von einem Command & Control-Server gesteuert werden. Anlass gibt mir dazu die Verarbeitungsgeschwindigkeit, mit der die Homebanking-Malware arbeitet und ich glaube nicht, dass damit ein menschlicher Man-in-the-Middle mithalten könnte. Auch die Funktionsvielfalt, mit der sich Homebanking-Trojaner auf verschiedene Banken und zum Beispiel der Bundespolizei-Trojaner auf verschiedene Länder einstellen lässt eigentlich nur den Schluss zu, dass diese Variablen nicht von der Malware selber transportiert, sondern von einem C & C abgerufen werden.

Um diese Malware zu betreiben, bedarf es deshalb seitens der Täter nur ihrer Verbreitung, die

[176] Fischer ebenda; das gilt auch für § 17 UWG.

sich im Ergebnis als Computersabotage in Tateinheit mit dem Ausspähen von Daten darstellt, und der Bereitstellung eines C&C, der die Kontodaten und neu generierten Seiten zuliefert. Es handelt sich im Ergebnis um einen einzigen Handlungsakt, der (in aller Regel) mit der Verbreitung der Malware abschließt. Mit anderen Worten: Die Täter handeln nur im Vorbereitungsstadium und begehen damit einen beendeten Versuch (wie beim Zünden einer Zeitbombe), von dem sie nur noch mit tatkräftigem Zutun zurücktreten können [177].

Die massenhafte Verbreitung dieser Malware legt gewerbsmäßiges Handeln nahe, die Wiederholung der Verbreitung mit verbesserten und aufgerüsteten Malwareversionen bandenmäßiges Handeln. Nur schon gewerbsmäßiges Handeln führt zu einem Anwendungsfall des besonders schweren Computerbetruges (§ 263a Abs. 2 in Verbindung mit § 263 Abs. 3 Nr. 1 StGB), der mit Freiheitsstrafe von sechs Monaten bis zu zehn Jahren droht. Die Kombination beider subjektiven Qualifikationen führt nach § 263a Abs. 2 in Verbindung mit § 263 Abs. 5 StGB zu einem gewerbsmäßigen Bandencomputerbetrug, der zu einem selbständigen Verbrechen ausgestaltet ist.

Das hat erhebliche Auswirkungen, weil wegen dieses Verbrechenstatbestandes die Beteiligungsformen durch § 30 StGB mit der Folge erweitert werden, dass bereits die Planung und Vorbereitung (Vorbereitung der Spam-Mails, Aquise des Botnetzes, Einrichtung des C&C) unter der Strafdrohung der Verabredung eines Verbrechens des gewerbsmäßigen Bandencomputerbetruges stehen, und die reicht von drei Monaten bis sieben Jahre und sechs Monate Freiheitsstrafe (§ 49 StGB), ohne dass bereits ein Erfolg eintreten sein muss.

Dasselbe Ergebnis folgt aus der gewerbs- und bandenmäßigen Fälschung beweiserheblicher Daten nach § 269 Abs. 3 in Verbindung mit § 267 Abs. 3, Abs. 4 StGB. Auch insoweit sind besonders schwere Fälle und ein selbständiger Verbrechenstatbestand vorgesehen.

2.4.6 verteilte Angriffe

Die Dienstverweigerung – Denial of Service – DoS – ist das Ergebnis einer Überlastung eines Web- oder anderen Servers infolge von Serviceanfragen, die er in dieser Masse nicht abarbeiten kann. Dazu reicht es bereits, immer wieder dieselbe (unsinnige) Serviceanfrage an einen Zielrechner zu richten, ohne überhaupt eine Antwort abzuwarten. Das Bemühen des Zielrechners um ordnungsgemäße Beantwortung kann zu seiner Überlastung führen, so dass er ganz ausfällt. Werden die Serviceanfragen von verschiedenen Stellen gleichzeitig ausgeführt, dann spricht man von einem (verteilten) Distributed Denial of Service – DDoS.

Botnetze sind für DDoS-Angriffe besonders geeignet. Sie verfügen über eine Vielzahl von Zombies, die allein mit der Menge ihrer gleichzeitigen Anfragen einen Zielrechner in die Knie zwingen können. Während die Anfragen eines oder weniger Geräte verhältnismäßig einfach anhand ihrer Internetadresse blockiert werden können, gelingt das bei Botnetzen nicht, weil die Zombies über sehr verschiedene und breit gestreute IP-Adressen verfügen, die zudem meistens aus den vertrauenswürdigen Netzen bekannter Zugangsprovider stammen. Wenn der Angriff vom Botnetz darüber hinaus kaskadiert wird, also wenn sich verschiedene Gruppen von Zombies beim „Feuern“ abwechseln, hat der angegriffene Server so gut wie keine Chance, die Angriffe abzuwehren.

DDoS-Angriffe sind bereits gegen eine Vielzahl von gewerblichen Webservern geführt worden. Meistens reicht bereits ihre Ankündigung, um ein Schutzgeld zu erpressen (§ 253 Abs. 1 StGB). Im Grundtatbestand drohen dem Erpresser fünf Jahre Freiheitsstrafe, handelt er gewerbs- oder bandenmäßig, dann liegt ein besonders schweren Fall vor (§ 253 Abs. 4 StGB). Für dieses Vergehen drohen ein bis fünfzehn Jahre Freiheitsstrafe. Ein selbständiges Verbrechen sieht der Erpressungstatbestand nicht vor.

Die Ausführung von DDoS-Angriffen gegen ge-

[177] Einzelheiten zum Versuch und Rücktritt: Dieter **Kochheim**, Die goldene Brücke. Gescheiterte Taten, Rücktritt vom Versuch und Straffreiheit, 18.01.2012

werbliche Internetveranstalter ist ein Standardfall der schweren Computersabotage gemäß § 303b Abs. 2 StGB (höchstens fünf Jahre Freiheitsstrafe) und in aller Regel ein besonders schwerer Fall gemäß § 303b Abs. 4 StGB, weil die Täter entweder *einen Vermögensverlust großen Ausmaßes* herbeiführen (Nr. 1) oder gewerbsmäßig handeln (Nr. 2), so dass ihnen sechs Monate bis zu zehn Jahre Freiheitsstrafe drohen. Einen eigenen Verbrechenstatbestand kennt auch die Computersabotage nicht.

Die fehlenden Verbrechenstatbestände sind den Herkünften der beiden Grundtatbestände geschuldet, passen aber nicht in das Gesamtbild, das vom digitalen Betrug (Computerbetrug, § 263a StGB) und von der digitalen Urkundenfälschung (Fälschung beweiserheblicher Daten, § 269 StGB) gezeichnet wird. Die Computersabotage hat ihre Wurzeln im Sachbeschädigungsrecht, was verständlich macht, dass die Zerstörung von Gegenständen gegenüber der Gewalt gegen Personen und personenbezogenen Rechten zurücktritt. Die schwerste Form der Erpressung ist dem Raub (§ 249 Abs. 1 StGB) und seinen schlimmen Steigerungsformen angepasst (räuberische Erpressung, § 255 StGB). Das zeigt, dass der Gesetzgeber wegen der Nötigungsmittel die körperliche Gewalt und nicht das existenziell gefährdete Vermögen vor Augen hatte.

Das Beispiel zeigt auch, dass das IuK-Strafrecht keine gleichförmigen Konturen hat, weil seine einzelnen Tatbestände an vorhandene, in sich geschlossenen Abschnitten angekoppelt wurden. Wegen der DDoS-Angriffe führt das dazu, dass sie keine Strafbarkeit wegen einer Verbrechensabrede kennen, weil es hier kein verfolgbares Verbrechen gibt.

2.4.7 Konsole

Jeder Zombie kann von den Botnetz-Betreibern über eine Backdoor als Konsole missbraucht werden. Das heißt, dass der Angreifer den Anwender verdrängen und den Zombie zu jeder Kommunikation oder Aktion im Internet missbrauchen kann. Er handelt unter der Identität des Anwenders und kann alle möglichen Formen der Kriminalität begehen, die denkbar sind.

2.4.8 Interlog: Klaus Störtebecker

Von zeitgeschichtlicher Bedeutung ist das Urteil des LG Düsseldorf aus 2011 gegen "Klaus Störtebeker", so der Alias des Täters [178]. Wer noch Zweifel an der Existenz der Cybercrime hatte, wird hier eines Besseren belehrt:

- Cyber-Kriminelle nutzen alle Möglichkeiten der Verschleierung und Tarnung,
- sind in Deutschland aufgewachsen und hier tätig,
- führen DDoS-Angriffe mit Botnetzen aus und
- drohen mit DDoS-Angriffen, um Schutzgeld zu erpressen,
- verlangen zur Verschleierung der Beutesicherung digitale Bons (Voucher) [179] und
- lassen deren Wert auf Kreditkarten auf Guthabenbasis übertragen,
- um dann die Beute am nächsten Geldautomaten abzuholen.

Der geständige Angeklagte hat mehrere Erpressungen und DDoS-Angriffe durchgeführt und sich dazu auf die Webseiten mehrerer Pferdewetten-Anbieter konzentriert. Das LG Düsseldorf hat ihn deshalb wegen gewerbsmäßiger Erpressung in Tateinheit mit Computersabotage zu einer Gesamtfreiheitsstrafe von zwei Jahren und zehn Monaten verurteilt. Beachtlich ist, dass das Gericht sowohl wegen der Erpressungen (§ 253 StGB) wie auch wegen der Computersabotagen (§ 303b StGB) von gewerbsmäßigem Handeln ausgegangen ist (§§ 253 Abs. 4, 303b Abs. 4 Nr. 2. StGB). Das sind keine Bagatellen mehr, die zur Nachsicht Anlass geben könnten.

Der Täter scheint ein typischer Vertreter der hiesigen Cybercrime-Szene zu sein: Junger Erwachsener, der dem Jugendrichter gerade entwachsen und mit allen Finessen vertraut ist, die in der Carding- und Hacking-Szene diskutiert und propagiert werden.

---

[178] **LG Düsseldorf**, Urteil vom 22.03.2011 - 3 KLs 1/11

[179] **CF**, Konvergenz auf dem Schwarzmarkt, 25.11.2010; **CF**, graue Bezahlsysteme, 08.12.2010.

2.5 Hacking

▸ Aurora, ▸ Night Dragon und ▸ Shady Rat geben professionelle Beispiele dafür, wie Malware quasi als Türöffner eingesetzt wird, um in fremde Computersysteme einzudringen, eine Backdoor zu installieren und dann „von Hand“ das System zu durchforsten, um Informationen zu stehlen. Das klassische Hacking kann auch auf anderen Wegen erfolgen. Schritt für Schritt, indem eine Schwachstelle gesucht wird, die als Sprungbrett für ein tieferes Eindringen in das System geeignet ist, durch gezieltes Zugehen auf Mitarbeiter und Einsatz von Sozialtechniken (Social Engineering) oder – auch ein schönes Beispiel – durch Verteilung von USB-Sticks als Werbegeschenke an Firmenmitarbeiter.

Das Hacking liefert das Leitbild für das IuK-Strafrecht im engeren Sinne mit den zentralen Strafvorschriften über das Ausspähen und Abfangen von Daten (§§ 202a Abs. 1, 202b StGB), dem Computerbetrug (§ 263a StGB) und schließlich die Datenveränderung (§ 303a StGB) und die Computersbotage (§ 303b StGB). Den Schwerpunkt des Hackings bilden gegenwärtig die Industrie- und Spionage im übrigen sowie der Hacktivismus im Zusammenhang mit politischen Auseinandersetzungen [180].

2.5.1 Spionage. Sabotage

Je mehr sich das Hacking auf die gezielte Informationsbeschaffung konzentriert, desto häufiger kommen auch andere Strafnormen in Betracht. Wegen der Geschäftsgeheimnisse ist auf § 17 Abs. 2 Nr. 1 lit a und b UWG hinzuweisen, wonach mit bis zu drei Jahren Freiheitsstrafe bestraft werden kann, *wer ... aus Eigennutz, zugunsten eines Dritten oder in der Absicht, dem Inhaber des Unternehmens Schaden zuzufügen, sich ein Geschäfts- oder Betriebsgeheimnis durch … Anwendung technischer Mittel* <oder> *Herstellung einer verkörperten Wiedergabe des Geheimnisses … unbefugt verschafft oder sichert*.

Um was es dabei geht, hat das BVerfG eingängig beschrieben [181]: *Als Betriebs- und Geschäftsgeheimnisse werden alle auf ein Unternehmen bezogene Tatsachen, Umstände und Vorgänge verstanden, die nicht offenkundig, sondern nur einem begrenzten Personenkreis zugänglich sind und an deren Nichtverbreitung der Rechtsträger ein berechtigtes Interesse hat. Betriebsgeheimnisse umfassen im Wesentlichen technisches Wissen im weitesten Sinne; Geschäftsgeheimnisse betreffen vornehmlich kaufmännisches Wissen. Zu derartigen Geheimnissen werden etwa Umsätze, Ertragslagen, Geschäftsbücher, Kundenlisten, Bezugsquellen, Konditionen, Marktstrategien, Unterlagen zur Kreditwürdigkeit, Kalkulationsunterlagen, Patentanmeldungen und sonstige Entwicklungs- und Forschungsprojekte gezählt, durch welche die wirtschaftlichen Verhältnisse eines Betriebs maßgeblich bestimmt werden können*.

Der gewerbsmäßige Verrat unternehmerischer Geheimnisse und ihre Auslandsverwertung betrachtet § 17 Abs. 4 UWG als besonders schwere Fälle, die mit bis zu fünf Jahren Freiheitsstrafe bedroht sind. Richtet sich die Informationsbeschaffung auf Staatsgeheimnisse (§ 93 Abs. 1 StGB), greifen die Vorschriften über den Landesverrat

---

[180] Statt vieler Beispiele: Dieter **Kochheim**, Eskalationen, 20.02.2011, S. 15 (IT-Söldner im Kampfeinsatz)

[181] **BVerfG**, Beschluss vom 14. März 2006 - 1 BvR 2087/03, 2111/03, Rn 87.
Die unternehmerischen Geheimnisse unterliegen dem Schutz des Grundrechts auf die Berufswahl (Art 12 Abs. 1 GG).

und die Gefährdung der äußeren Sicherheit mit nachhaltigen Strafen [182]. Der Verrat illegaler Geheimnisse (§ 97a StGB) kann sich auch auf Wirtschaftsgeheimnisse, zum Beispiel aus dem Bereich der Rüstungsindustrie beziehen.

▸ Stuxnet hat die Anfälligkeit von industriellen Steuerungsanlagen gegenüber Cyberangriffe gezeigt und mehrere Ausfälle von Stromnetzen zeigen die Anfälligkeit kritischer Infrastrukturen [183]. Unternehmen oder Behörden, die keine Verbindungen zum Internet haben, sind eine absolute Ausnahme und es ist zu erwarten, dass Hacking-Angriffe künftig nicht nur zur Informationsbeschaffung, sondern auch zum gezielten Angriff gegen Konkurrenten und zur Erpressung durchgeführt werden. Auch auf dem ersten Blick ungewöhnliche Angriffe müssen in Betracht gezogen werden. So hat das Sicherheitsunternehmen McAfee jüngst vor Hackerangriffe gegen Autos und ihre eingebaute Elektronik gewarnt [184].

Die Vielzahl der möglichen Angriffsformen schließt eine Eingrenzung der betroffenen Straftatbestände aus dem IuK-Strafrecht im weiteren Sinne aus.

Übersicht: Landesverrat

Friedensgefährdende Beziehungen	§ 100 StGB
Geheimdienstliche Agententätigkeit	§ 99 StGB
Landesverrat	§ 94 StGB
Landesverräterische Agententätigkeit	§ 98 StGB
Landesverräterische Ausspähung, Auskundschaften von Staatsgeheimnissen	§ 96 StGB
Landesverräterische Fälschung	§ 100a StGB
Offenbaren von Staatsgeheimnissen	§ 95 StGB
Preisgabe von Staatsgeheimnissen	§ 97 StGB
Verrat illegaler Geheimnisse	§ 97a StGB
Verrat in irriger Annahme eines illegalen Geheimnisses	§ 97b StGB

[182] Siehe auch: **CF**, Frieden, Staatsschutz, öffentliche Ordnung, 2007

[183] Dieter **Kochheim**, Netzkommunikation, 10.07.2010, S. 27 (Heißer Cyberwar).

[184] Stuart **McClure** ua, Achtung: Malware voraus. Eine Analyse zukünftiger Gefahren für Fahrzeugsicherheitssysteme, McAfee 26.08.2011

2.5.2 Formenwandel

Die Erscheinungsformen im Zusammenhang mit dem ▸ Skimming zeigen besonders deutlich die Wandlungs- und Anpassungsfähigkeit der Täter. Das gilt besonders für das Skimming im engeren Sinne, also die Beschaffung der Kontodaten, um mit ihnen Zahlungskarten mit Garantiefunktion zu fälschen und vor allem beim Cashing zu missbrauchen (§§ 152a, 152b Abs. 1, Abs. 2, 263a Abs. 2, 263 Abs. 3, Abs. 5 StGB). Seine bekannteste Form besteht darin, die Daten vom Magnetstreifen mit Skimmern auszulesen und die PIN-Eingaben mit Kameras zu beobachten oder mit Tastaturaufsätzen abzugreifen.

Die Anfälligkeit des Magnetstreifens hat dazu geführt, dass der EMV-Chip verbindlich eingeführt und im europäischen Bankenverbund durchgesetzt wird, dass die Autorisierung nur anhand des EMV-Chips erfolgt [185]. Die Täter haben darauf reagiert:

▸ Sie verwenden elektronische Bauteile, die sie in die Geldautomaten einbauen und spähen damit den Datenstrom zwischen dem Lesegerät und der internen Elektronik aus [186]. Die Stromversorgung liefert der Geldautomat selber. Nur die Tastatureingaben können sie damit noch nicht auslesen, weil diese Daten auf dem Weg zwischen Tastatur und Elektronik verschlüsselt sind. Insoweit bestehen noch Chancen zur Innovation.

▸ Sie greifen nicht die Geldautomaten von Banken, sondern die Zahlungsterminals von Tankstellen an [187]. Es gibt Schätzungen, wonach der Skimming-Angriff Anfang 2011 gegen eine Tankstelle in Castrop-Rauxel einen Schaden in Höhe von fast 1 Mio. € verursacht hat [188].

▸ Das POS-Skimming wurde wieder belebt. Dazu werden die Zahlungsterminals im Einzelhandel mit einer zusätzlichen Elektronik ausgestattet, die im Innern des Terminals die Kartendaten abfängt, speichert und mit Nahfunktechnik an die Täter in der Kassenzone übermittelt. Eine flexible Platine wird zwischen die Tastatur und die Geräteelektronik gesetzt, die dafür sorgt, dass auch die PIN-Eingaben protokolliert werden [189]. Diese Methode hat mehrere Vorteile für die Täter: Eine fehlerfreie Aufzeichnung der PIN und die Verschaffung der EMV-Daten, die mit einem normalen Skimmer nicht ausgelesen werden können.

▸ Das Cashing verlagert sich immer mehr in das außereuropäische Ausland, vor allem nach Nordamerika, Afrika und in den Fernen Osten. Dort werden nur die Magnetstreifen der gefälschten Zahlungskarten ausgelesen, nicht aber der EMV-Chip. Das fälschungssichere MM wird außerhalb Deutschlands nicht geprüft [190].

▸ Für das schnell verdiente Taschengeld wird das ▸ Cash Trapping eingesetzt. Diese Form des Trickdiebstahls ist kinderleicht [191].

Der „typische“ Skimmingtäter lässt sich nach Geschlecht, Alter und Herkunft treffend beschreiben und vom „typischen“ Cardingtäter abgrenzen. In der Cardingszene [192] werden die Methoden beim Abgreifen von Kartendaten, ihrem Einsatz und die Beutesicherung ungeniert diskutiert und das Equipment sowie die Daten selber offen gehandelt. Das Cashing mit WhiteCards ist hier ebenfalls verbreitet, für die Datenbeschaffung werden hingegen eher Hacking-Methoden eingesetzt. Andere Kartendelikte mit optischen Fälschungen oder mit fremden Daten auf den Magnetstreifen

---

185 **CF**, eierlegende Wollmilchsau, 20.03.2011

186 Das ist dann tatsächlich ein Abfangen von Daten im Sinne von § 202b StGB.

187 Dieter **Kochheim**, Skimming, 22.04.2011, S. 8

188 Susanne **Linnenkamp**, Profis manipulierten SB-Tankstelle in Castrop-Rauxel, ruhrnachrichten.de 10.03.2011

189 Die Bilder, die ich gesehen habe, zeigen eine beachtliche handwerkliche Leistung.

190 **CF**, Sicherheitsmerkmale und Merkmalstoffe, 06.02.2010

191 Tatsächlich gibt es Hinweise darauf, dass strafunmündige Kinder für das Cash Trapping abgerichtet und eingesetzt werden.

192 Siehe Einleitung und Anhang zu: Dieter **Kochheim**, Verdeckte Ermittlungen im Internet, 27.07.2011, S. 5, 64.

werden hier ebenfalls propagiert und begangen [193].

Im Kasten <rechts> wird der Angriff gegen den Finanzdienstleister RBS World Pay angesprochen [194], mit dem wir zum Thema Hacking zurückkommen. Das Beispiel belegt, wie die Methoden des Hackings und des Cashings zusammengeführt werden können, wobei das Hacking nicht nur zum Ausspähen (§ 202a Abs. 1 StGB), sondern auch zur Manipulation der Kontoeinstellungen genutzt wurde (besonders schwerer Fall der schweren Computersabotage, § 303b Abs. 2, Abs. 4 Nr. 1 StGB; Fälschung beweiserheblicher Daten, § 269 StGB).

Die Beispiele belegen vor allem, dass die Cybercrime einem ständigen Formenwandel unterlegen ist und sich Erscheinungsformen mischen. Gleichwohl lassen sich immer wieder phänomenologische Grundformen erkennen wie das Hacking als solches (Eindringen in fremde Rechnersysteme), der Einsatz von Malware und ihre automatische Steuerung durch Command and Control-Server – C&C – sowie das Cashing. Diese Grundformen lassen sich auch strafrechtlich „begreifen“, so dass eine völlige Neubewertung nur selten erforderlich ist. Die Normen des IuK-Strafrechts mögen nicht immer schlüssig, vollständig und systematisch stimmig sein. Dennoch deckt es die meisten Anwendungsfälle ab.

Das ändert nichts am der Tatsache, dass das IuK-Strafrecht hohe Anforderungen an die Strafverfolger stellt, weil sie nur auf wenige Erfahrungstatsachen und geklärte Rechtsfragen zurückgreifen können, technische und wirtschaftliche Prozesse

Besonders heimtückisch gingen die Hacker vor, die Ende 2008 in die Datenhaltung einer US-amerikanischen Bank eindrangen und die Kartendaten einschließlich PIN von 100 Kunden ausspähten. Gleichzeitig erhöhten sie deren Auszahlungslimit. Am 08.11.2008 wurden weltweit und gleichzeitig an 130 Geldautomaten in 49 Städten die gefälschten Zahlungskarten eingesetzt und damit 9 Millionen US-$ erbeutet.

Dieter **Kochheim**, Skimming, 22.04.2011, S. 8

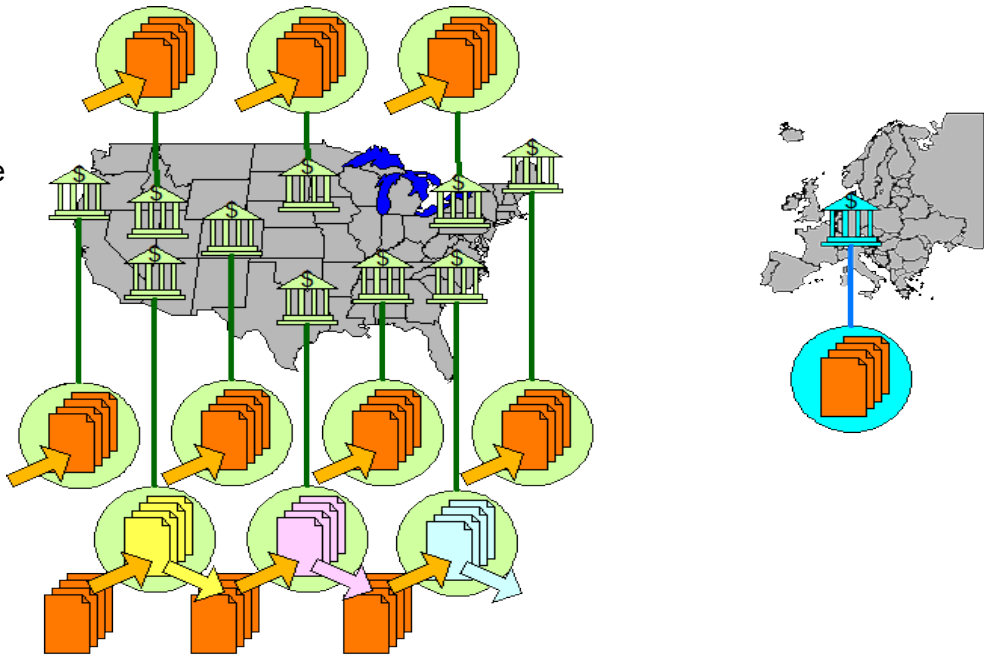
begreifen und das bestehende Recht darauf an wenden müssen.

---

[193] Beide Erscheinungsformen, Fälschung der optischen Sicherheitsmerkmale einer Zahlungskarte oder Fälschung der Daten auf dem Magnetstreifen, sind Verbrechen gemäß § 152b Abs. 1 StGB. Da sich die Garantiefunktion einer Zahlungskarte nur darauf bezieht, dass sie von Dritten zur Zahlungsabwicklung akzeptiert wird, können auch die Karten von Verbundsystemen wie Tankkarten oder Pay-Back-Karten Zahlungskarten mit Garantiefunktion sein.

[194] Kriminelle stehlen 9 Millionen Dollar in weltweitem Coup, Heise online 06.02.2009

2.5.3 Kursmanipulation



Bei der klassischen Aktienkursmanipulation erwirbt der Täter zunächst Penny-Stocks, andere handelsfähige Wertpapiere oder Rechte zu einem kleinen Preis und versucht dann mit Spam-Aktionen und anderer gezielter Öffentlichkeitsarbeit Käufer für diese Aktien zu gewinnen. Je mehr er zum Kauf überredet, desto höher steigt der Marktpreis und damit der Depotwert der Aktien des Täters. Zur passenden Zeit verkauft er seine Aktien zu dem gepushten Preis.

Seit 2008 wird eine Variante diskutiert, die nicht auf Werbung, sondern auf Hacking basiert. Sie zeigt besondere Raffinesse seitens der Täter und die Grenzen des Strafrechts auf [195].

Zunächst muss der Täter auch bei dieser Methode investieren, indem er ein Aktienpaket mit Penny-Stocks erwirbt und vom Ausland aus in ein Aktiendepot in Deutschland stellt <Grafik, blau unterlegt>. Danach startet er eine groß angelegte Aktion in den USA, bei der er die Aktiendepots von Bankkunden missbraucht. Die einlagernden Wertpapiere verkauft der Täter und erwirbt dafür genau die Penny-Stocks der Sorte, die er vorher selber eingekauft hat <hellgrün unterlegt>.

Je mehr Depots er auf diese Weise missbraucht, desto höher steigt der Kurs der Aktien und damit auch der Kurswert seines Depots. Sobald der Einkauf der Aktien den Grad der Marktsättigung und der Kurs den höchstmöglichen Stand erreicht haben, verkauft der Täter seinen eigenen Wertpapierbestand - an eines der von ihm missbrauchten USA-Depots und mit höchsten Gewinn. Diesen streicht er ein, indem er das eigene Depot in Deutschland auflöst. In den USA verlieren die manipulierten Depots darauf ganz erheblich an Wert. Die meisten dürften dann auf fast Null gefahren sein.

Dieses Beispiel zeigt die fatale Folge davon, dass im Bereich der Cybercrime die Täter zwar international agieren, die Rechtsordnungen jedoch an den nationalstaatlichen Grenzen enden. Selbst wenn man auf das Beispiel vollständig das deutsche Strafrecht anwenden könnte, wären die Einrichtung, der Betrieb und die Auflösung des Aktiendepots in Deutschland - für sich allein betrachtet - nicht strafbar.

Die Manipulationen in den USA wären nach deutschem Recht als Computerbetrug (§ 263a StGB) und Fälschung beweiserheblicher Daten (§ 269 StGB) strafbar. Der Handlungsort und alle anderen eine örtliche Zuständigkeit begründenden Umstände sind im Ausland angesiedelt, so dass die Strafverfolgung in Deutschland nicht zulässig ist.
Die Wertsteigerung des Aktiendepots in Deutschland begründet keinen Erfolgsort im Sinne von § 7 Abs. 1 StPO. Das liegt daran, dass die Strafvorschrift über den Betrug (§ 263 StGB) und ihr folgend für den Computerbetrug (§ 263a StGB) nach einer Stoffgleichheit zwischen den Vermögensschäden, die durch die Manipulationen in den USA entstanden sind, und dem Vermögenszuwachs verlangen, den er erlangt hat.

Daran fehlt es aus zwei Gründen. Der Wertverlust in den USA tritt erst ein, nachdem der Täter seinen Aktienbestand verkauft hat und er weitere

[195] Das Kapitel wurde übernommen aus: Dieter **Kochheim**, Cybercrime, 24.06.2010, S. 53 (Aktienkursmanipulation).

Kursmanipulationen in den USA unterlässt. Die Stoffgleichheit verlangt hingegen, dass ein Vermögensnachteil auf der einen Seite unmittelbar zu einem Vermögensvorteil auf der anderen Seite führt.

Außerdem erfolgt die Wertsteigerung im deutschen Depot nicht dadurch, dass Zahlungen eingehen, sondern dadurch, dass der Tauschwert an der Börse gestiegen ist. Der Wertzuwachs gründet also auf einem Tauschmechanismus, auf den der Täter zwar mittelbar (durch immer neue Kaufnachfragen) Einfluss genommen, den er aber nicht unmittelbar beeinflusst hat. Somit fehlt es an der Stoffgleichheit.

2.6 Betrug. Webshops. Abofallen

Die Massenkriminalität im Internet ist Betrugskriminalität. Das zeigt vor Allem das Carding. In den einschlägigen Carding-Boards werden nicht nur ausgespähte Kontozugangsdaten, Malware und Skimming-Equipment gehandelt, sondern auch Bankkonten unter falschen Namen, Paketstationen, gefälschte Personalpapiere, Führerscheine und Diplome sowie Anleitungen zu betrügerischen Warenkäufen. Die Betreiber (Administratoren und Moderatoren) verdienen dabei an den Zugangsgebühren, an Monopollizenzen (zum Beispiel auch zum Verkauf von Rauschgift oder Waffen) und an den Treuhandgebühren, die sie als Abwickler von Käufen erhalten.

Die damit verbundene Kriminalität ist in erster Linie klassisch: Betrug (§ 263 StGB) und Urkundenfälschung (§ 267 StGB [196]). Sie haben einige rechtliche Besonderheiten, die es vorzustellen gilt, auch wenn sie nicht dem IuK-Strafrecht als solches zuzurechnen sind.

2.6.1 Kontoeröffnungsbetrug [197]

Als Kontoeröffnungsbetrug wird die Einrichtung eines Bankkontos unter falscher Identität und Vorlage falscher Urkunden mit dem Ziel angesehen, die Bank zu Zahlungen zu veranlassen, die weder durch Guthaben noch durch den Zahlungswillen des Kontoinhabers gedeckt sind. Die rechtlichen Konstellationen, die daraus entstehen, sind nicht so einfach, wie man auf dem ersten Blick meint.

Die übliche Masche wurde Anfang 2012 vom BGH beschrieben [198]: Der Angeklagte fälschte *insbesondere Anmeldebestätigungen und Verdienstbescheinigungen, unter deren Vorlage jeweils zunächst ein Bankkonto eröffnet wurde. Später wurde - ebenfalls unter Vorlage falscher Urkunden - ein Kreditvertrag abgeschlossen bzw. ein Finanzierungsgeschäft getätigt* <Rn 2>.

Die erste Tathandlung - das noch nicht betrügerische Eröffnen eines Kontos unter Gebrauch falscher Urkunden - ist keine selbständige Tat <Rn 4>: *Wird eine gefälschte Urkunde dem ursprünglichen Tatplan entsprechend mehrfach gebraucht, liegt indes nur eine Urkundenfälschung vor*.

Die Fälschung einer Urkunde und ihr planmäßiger Gebrauch in mehreren Fällen führt zu einer deliktischen Einheit und somit zu einer einheitlichen Tat (§ 52 StGB) der Urkundenfälschung (§ 267 StGB). Beim Kontoeröffnungsbetrug führt das zu einer weiteren Verbindung mit dem Ziel der Vermögensschädigung der Bank. Es handelt sich dann um eine Tat des Betruges in Tateinheit mit Urkundenfälschung (§§ 263, 267, 52 StGB).

Die rechtlichen Schwierigkeiten entstehen immer beim Blick auf die Details. Deshalb betrachten wir die einzelnen Tatschritte, wobei das Ziel des Täters darin besteht, unter einer falschen Identität einen Kredit von der Bank ausgezahlt zu bekommen (das ist beim Finanzierungsbetrug nicht anders: Hier erlangt der Täter statt der Geldzahlung die finanzierte Ware).

2.6.1.1 Kontoeröffnung und Verfügungen unter einer Legende

Die beliebtesten gefälschten Urkunden sind Personalpapiere (Ausweise, Pässe, Identitätskarten), Meldebescheinigungen (die kann man auch "in echt" bekommen, wenn man sich unter Vorlage des falschen Ausweises beim Einwohnermeldeamt anmeldet), und Gehaltsbescheinigungen (auch "Lohntüten") und ausländische Führerscheine. Die Herstellung der Fälschungen ist strafbar (§ 267 StGB).

Wird unter falschen Personalien ein reines Guthabenkonto eröffnet, dann ist das nur als Urkundenfälschung strafbar nach § 267 StGB (Gebrauch einer falschen Urkunde). Auch der Täter, der unter einer falschen Identität agiert, ist kontoberechtigt [199]: *Berechtigter Karteninhaber ist aber auch derje-*

---

[196] Siehe auch oben: Urkunde und Abbild.

[197] Das Kapitel über den Kontoeröffnungsbetrug wurde im März 2012 neu eingefügt. Siehe auch: CF, Kontoeröffnungsbetrug, 18.03.2012.

[198] **BGH**, Beschluss vom 07.02.2012 - 3 StR 406/11

[199] **BGH**, Beschluss vom 21.11.2001 - 2 StR 260/01, Rn

nige, der die Überlassung der Karte unter Täuschung über seine Identität vom Kartenaussteller erlangt hat.

Dies betrifft vor Allem die Täter, die unter einer falschen Identität leben, sich ihre Legende einrichten und dazu auch Verträge für den täglichen Bedarf schließen. Sie achten meistens sorgsam darauf, dass jedenfalls ihre Legende schuldenfrei bleibt. Lässt sich für den Zeitpunkt der Kontoeröffnung kein Zahlungsunwille und keine Täuschung über die Zahlungsfähigkeit des Kunden feststellen, dann liegt kein Betrug vor (§ 263 StGB) [200]. Entschließt sich der Kunde später dazu, das Konto zu missbrauchen, dann ist nach der Art seiner Verfügung zu unterscheiden.

Setzt der Täter eine Zahlungskarte in Schädigungsabsicht am Geldautomaten der Karten ausgebenden Bank ein, begeht er weder einen Computerbetrug (§ 263a StGB) [201] noch einen Missbrauch von Scheck- und Kreditkarten im Sinne von § 266b StGB [202]. Er bleibt straffrei.

Setzt der Täter eine Zahlungskarte in Schädigungsabsicht am Geldautomaten einer anderen Bank ein, dann macht er sich nach § 266b StGB strafbar. Diese Spezialvorschrift verdrängt den Betrug [203].

Setzt der Täter eine Zahlungskarte in Schädigungsabsicht im Lastschriftverfahren ein (Point of sale ohne Zahlungsgarantie - POZ) begeht er einen Betrug zum Nachteil des Akzeptanten (§ 263 StGB) [204].

8.

[200] Kurzsachverhalt ohne Gründe: **BGH**, Beschluss vom 11.10.1988 - 1 StR 486/88.

[201] **BGH**, Beschluss vom 21.11.2001 - 2 StR 260/01, 1. Leitsatz.

[202] Ebenda, 2. Leitsatz.

[203] Ebenda, Rn 11. In dem Fall, dass der Kunde bei der Kontoeröffnung über seine Zahlungsbereitschaft und -fähigkeit trog, kann hierdurch ein Betrug zum Nachteil der Karten ausgebenden Bank in Tateinheit mit Scheckkartenmissbrauch eintreten (§§ 263, 266b, 52 StGB); ebenda, Rn 23.

[204] **BGH**, Beschluss vom 21.11.2001 - 2 StR 260/01, Rn 36.

2.6.1.2 Urkundendelikte

Kopien und offensichtliche Abbilder von Urkunden können nicht als falsche Urkunde gebraucht werden. Es bedarf immer einer verfälschten oder gefälschten Urkunde, die im Rechtsverkehr vorgelegt wird [205]. Fälschung und Gebrauch bilden eine mehraktige, aber einheitliche Tat. Der mehrfache Gebrauch derselben gefälschten Urkunde führt in aller Regel ebenfalls zu einer einheitlichen Tat [206].

Die Herstellung von auf den Besteller abgestimmter Papiere macht häufig dessen Mitwirkung nötig (Benennung der Personalien, Passbild). Dadurch wird er nicht nur zum Anstifter (§ 26 StGB), sondern auch zum Gehilfen (§ 27 StGB). Die Anstiftung ist aber die intensivere Form der Teilnahme und verdrängt deshalb die Beihilfe.

Unabhängig von dem Fälschungsdelikt ist auch die Verwahrung falscher (in- und ausländischer) Ausweise, Aufenthaltspapiere und Fahrzeugpapiere strafbar, wenn sie im Rechtsverkehr verwendet werden sollen (§§ 276, 276a StGB).

2.6.1.3 Eröffnung eines Debitkontos

Reine Guthabenkonten können im Verhältnis zum Kontoinhaber beim führenden Finanzdienstleister keinen Schaden verursachen. Dazu müsste er aus eigenem Vermögen Zahlungen an Dritte leisten, die nicht durch Einlagen gedeckt sind. Kontoeinrichtungs- und -führungsgebühren führen nicht zu einem Vermögensgewinn beim Kontoinhaber. Sie sind reine Folge- und keine Tatschäden im Sinne des Betrugstatbestandes (§ 263 StGB).

Die schlichte Eröffnung eines Debitkontos unter Vorlage falscher Personalpapiere ist deshalb kein Betrug, sondern nur der Gebrauch falscher Urkunden und deshalb eine Urkundenfälschung gemäß § 267 StGB.

[205] Siehe oben: Urkunde und Abbild. Zuletzt: **BGH**, Beschluss vom 17.11.2011 - 3 StR 203/11, Rn. 10.

[206] **BGH**, Beschluss vom 07.02.2012 - 3 StR 406/11

2.6.1.4 Einrichtung eines Kreditkontos ohne Kontobelastung

Die Einrichtung eines Kontokorrentkontos mit der Zusage eines Überziehungskredits räumt dem Täter die Option ein, das Konto im Rahmen des Limits zu missbrauchen. Mit der schadensgleichen Vermögensgefährdung hat die Rechtsprechung die Tatvollendung vorverlagert. Damit würde die Schaffung der Option seitens der Bank ausreichen, dass der Täter den Betrug vollendet hat Diese Konstruktion steht aber zunehmend unter Kritik und nach einzelnen Stimmen in Rechtsprechung ist sie sogar entbehrlich.

Das BVerfG hat die schadensgleiche Vermögensgefährdung zunächst bestätigt [207], verlangt jetzt aber nach einer rechnerischen Bezifferung und Darlegung eines Mindestschadens [208]. Das sind strengere Anforderungen als die zur klassische Begründung des Gefährdungsschaden [209]. Der BGH zeigt eine uneinheitliche Rechtsprechung. Am deutlichsten geworden ist 2011 der 3. Strafsenat des BGH, der an die Stelle des Gefährdungsden Eingehungsschaden setzte [210].

Diese feinsinnige Unterscheidung löst die Anwendungsproblem aber auch nicht ganz. Der Eingehungsschaden ergibt sich danach aus der rechnerischen Gegenüberstellung der wirtschaftlichen Werte der gegenseitigen vertraglichen Ansprüche beim Vertragsabschluss selber. Gemeint ist der Vergleich der wirtschaftlichen Werte der beiderseitigen Vertragspflichten nach einer noch abstrakten Berechnung.

Deshalb bleibt die Frage, ob allein schon durch die irrtumsbedingte Einräumung eines Überziehungskredites ein Eingehungsschaden entsteht, wenn auf der Passivseite ein wertloser Forderungsanspruch entstehen würde.

2.6.1.5 Gefährdungsschaden beim Überziehungskredit

Die Vermögensverfügung im Zusammenhang mit der Gewährung eines Überziehungskredits erfolgt bei der letzten intellektuellen Prüfung, ob er gewährt wird. Die Rechtsprechung hat aber immer wieder davon abgesehen, bereits auf seine Bewilligung abzustellen [211]. Jedenfalls mit dem Zugang der Scheckkarte tritt die Vermögensgefährdung ein, sagte der BGH im Jahr 2001 [212]:

Insoweit hat die Angeklagte unter Vorlage des gefälschten Personalausweises und Täuschung über ihre Zahlungswilligkeit bei der Postbank die Eröffnung eines Kontos sowie die Übergabe von Schecks und einer Kreditkarte erreicht. Zudem hat sie ... auch die in den Fällen II. 10. und 12. eingesetzte ec-card erlangt. Sie ist daher vom Landgericht zu Recht wegen Betrugs in Tateinheit mit Urkundenfälschung verurteilt worden. Der Betrug war mit der Aushändigung der Schecks und der ec-card sowie der Kreditkarte an die zahlungsunwillige Angeklagte vollendet, da dadurch eine konkrete Vermögensgefährdung eingetreten ist (...).

Daran hat der BGH auch in jüngerer Zeit festgehalten [213]. Das dürfte auch für eine Entscheidung aus dem Jahr 2008 gelten [214], in der ebenfalls die Verurteilung des Angeklagten wegen Betrug und Urkundenfälschung in Tateinheit referiert wird. Näher ausgeführt wird aber nur zum

---

207 CF, Schaden und schadensgleiche Vermögensgefährdung, 31.01.2010; **BVerfG**, Beschluss vom 10.03.2009 - 2 BvR 1980/07.

208 CF, Bezifferung und Darlegung eines Mindestschadens, 08.01.2012; **BVerfG**, Beschluss vom 07.11.2011 - 2 BvR 2500/09, 1857/10, Rn 162 ff.

209 CF, BVerfG: Bezifferter Gefährdungsschaden, 15.08.2010; **BVerfG**, Beschluss vom 23.06.2010 - 2 BvR 2559/08, 105/09, 491/09.

210 CF, Der Eingehungsschaden löst den Gefährdungsschaden ab, 16.02.2011; **BGH**, Beschluss vom 07.1.2010 - 3 StR 433/10; die Entscheidung ist vom Gegenstand her identisch mit: **BGH**, Beschluss vom 07.1.2010 - 3 StR 434/10.

211 **BGH**, Beschluss vom 21.11.2001 - 2 StR 260/01, Rn 31.

212 Ebenda, Rn 21. Die als Gegenmeinung angegebene Quelle (**BGH**, Beschluss vom 11.10.1988 - 1 StR 486/88) betrifft eher die Frage nach der Täuschung als nach dem Schadenseintritt.

213 **BGH**, Beschluss vom 14.10.2010 - 2 StR 447/10, Rn 3.

214 **BGH**, Beschluss vom 11.12.2008 - 5 StR 536/08

Betrug, zu der Täuschung im Zusammenhang mit Inhaber- oder Ordenschecks <Rn 7> und schließlich zur Frage der Tatvollendung <Rn 10>: Nach Vorlage eines falschen Schecks schrieb die Bank dem Konto die Valuta gut. Damit ist der Betrug vollendet und das Versuchsstadium abgeschlossen. Beendet wird die Tat aber erst durch die Auszahlung an den Täter. Erlangt er zunächst nur einen Teilbetrag der Gutschrift, dann dauert das Beendigungsstadium weiter an. Mehrere Abhebungen werden dadurch zu einer einheitlichen Tat [215].

Ungewöhnlich ist jedoch ein Beschluss aus dem Jahr 2011 formuliert [216]: Er berichtet von einem *überregional operierenden Kontoeröffnungsbetrügerring*, in dem dem Angeklagten die Aufgabe zukam, "Läufer" für die finale Tatausführung zu rekrutieren <Rn 3 bis 5>. Es ging schließlich um 14 Kontoeröffnungen unter falschen Identitäten und die Verurteilung des Angeklagten wegen 14 Fälle der Urkundenfälschung wird vom BGH nicht beanstandet. Erfolgreich in ihrem Sinne waren die Täter aber nur in 2 Fällen, wo es es zur Auszahlung von 10.000 und 5.000 Euro kam. Der BGH beanstandet, dass in beiden Fällen trotz des deutlichen Wertunterschiedes dieselbe Einzelstrafe ausgeurteilt wurde <Rn 9>. Wenn auf die Wertigkeit des Erlangten abgestellt wird, dann sollte man meinen, es gehe um Betrug. Davon ist in dem Beschluss aber keine Rede, sondern nur von Urkundenfälschung.

Klare Absagen an den Schadenswert von Überziehungszusagen gibt es jedenfalls nicht. Zu den Anforderungen an ihn gibt es noch keine gefestigte Rechtsprechung und auf den Eingehungsschaden ist nur eine weitere Entscheidung im Zusammenhang mit der Schadensfeststellung bei betrügerischer Kapitalerhöhung eingegangen, die nicht weiter hilft [217]: *Ein Schaden liegt demnach vor, wenn die von dem Getäuschten eingegangene Verpflichtung wertmäßig höher ist als die ihm dafür gewährte Gegenleistung unter Berücksichtigung aller mit ihr verbundenen, zur Zeit der Vermögensverfügung gegebenen Gewinnmöglichkeiten (...). Zu berücksichtigen ist beim Eingehen von Risikogeschäften dabei auch eine täuschungs- und irrtumsbedingte Verlustgefahr, die über die vertraglich zugrunde gelegte hinausgeht.*

2.6.1.6 Bilanzielle Wirkung des Kredits

Unter strenger Betrachtung hat die Gewährung eines Überziehungskredits keine bilanzielle Auswirkung, solange er nicht in Anspruch genommen wird. Bei seiner regulären Abwicklung würde sich ein bilanzieller Passivtausch ergeben: Per Forderungen (gegen den Kunden) an Kasse (Auszahlung, Überweisung). Beim böswilligen Kunden fehlt die Chance der Realisierung für die Forderung, der Kassenwert vermindert sich zulasten der Passivsumme und verringert den Gewinn. Dem könnte die Bank gegensteuern, wenn sie bereits bei der Kreditgewährung eine Rücklage in gleicher Höhe bilden würde. Aber auch das schmälert den Gewinn.

Für diese Fälle hat der 3. Strafsenat einen radikalen Vorstoß gemacht: Die signifikante Erhöhung der Leistungswahrscheinlichkeit [218]. Sie hat das Gericht angenommen, wenn die Täter Lebensversicherungen abschließen in der festen Absicht, binnen kurzer Zeit mit gefälschten Todesbescheinigungen die Versicherungssummen einzufordern. Das bringt alle auf langfristige Laufzeit und gestreutes Risiko angelegte Kalkulationen der Versicherung durcheinander und hätte den eingangs beschriebenen Effekt. Deswegen soll *der Schaden bei den getäuschten Versicherungsunternehmen nicht erst mit Auszahlung der jeweiligen Versicherungsleistung, sondern bereits mit Abschluss der Versicherungsverträge* eintreten <Rn 144>. Die dagegen gerichtete Kritik befürchtet, dass da-

---

[215] Zum Betrug mit gefälschten Überweisungsträgern: **BGH**, Urteil vom 18.06.2008 - 2 StR 115/08.

[216] **BGH**, Beschluss vom 29.06.2011 - 1 StR 136/11

[217] **BGH**, Beschluss vom 14.04.2011 - 2 StR 616/10, Rn 12.

[218] CF, Erhöhung der Leistungswahrscheinlichkeit, 31.01.2010; **BGH**, Urteil vom 14.08.2009 - 3 StR 552/08.

mit jeder böswillige Kunde zum Betrüger wird [219] und tatsächlich ist die Diskussion um signifikante Erhöhung der Leistungswahrscheinlichkeit nicht wieder aufgenommen worden.

Der Gedanke bekommt neues Gwicht unter folgendem Gesichtspunkt: Der normale bargeldlose Zahlungsverkehr ist ein völlig automatisierter Vorgang. Die Rechenzentren der Banken prüfen neben der Authentizität grundsätzlich nur das Kontoguthaben, den Überziehungskredit und einige andere Einschränkungen (Auslandsverfügung, Tages- und Wochenlimit). Daneben laufen unterschiedliche Routinen, die auffällige Verfügungen herausfiltern (zum Beispiel ungewöhnlicher Betrag, Verfügung ins Ausland, mehrere Verfügungen am Geldautomaten nacheinander), die sie zu einer intellektuellen Prüfung und womöglich Nachfrage veranlassen [220].

Im Zusammenhang mit ärztlichem Abrechnungsbetrug hat der BGH gerade jetzt wieder festgestellt [221]: *Bei Betrugsvorwürfen im Zusammenhang mit standardisierten, auf Massenerledigung angelegten Abrechnungsverfahren ist nicht erforderlich, dass der jeweilige Mitarbeiter hinsichtlich jeder einzelnen geltend gemachten Position die positive Vorstellung hatte, sie sei der Höhe nach berechtigt; vielmehr genügt die stillschweigende Annahme, die ihm vorliegende Abrechnung sei insgesamt „in Ordnung". Daher setzt ein Irrtum nicht voraus, dass tatsächlich eine Überprüfung der Abrechnungen im Einzelfall durchgeführt wurde* [222].

Folgt man diesem Gedanken, dann stellt sich das Bild anders dar: Im bargeldlosem Zahlungsverkehr findet die letzte Prüfung der Kreditwürdigkeit zusammen mit der Entscheidung über die Eingabe des Limits in die EDV der Bank statt. Sie verliert damit - jedenfalls im unauffälligen Massenverkehr - die Kontrolle über ihre Vermögensrisiken. Während im üblichen Zahlungsverkehr ein Ausfallrisiko bei wenigen Prozent besteht, ist das bei Betrügern anders und schnellt auf bis zu 100 Prozent des Überziehungskredits hoch.

Das rechtfertigt es jedenfalls in den Fällen des Kontoeröffnungsbetruges, wo mit falschen Urkunden der Überziehungskredit ertrogen wird (Arbeitsverträge, Gehaltsbescheinigungen) von einem Gefährdungs- oder Eingehungsschaden auszugehen, der zu einem vollendetem Betrug führt (§§ 263 StGB).

2.6.1.7 Einrichtung eines Finanzierungskontos

Beim Finanzierungskonto geht es darum, einen Warenkauf durch einen Bankkredit zu finanzieren. In diesen Fällen händigt das Warenhaus den Gegenstand aus und tritt die Bank im Innenverhältnis für den Kaufpreis ein. Mit der Aushändigung der Ware wird der Betrug vollendet. Finanzierungskäufe unter Verwendung falscher Identitäten und Urkunden und gleichzeitiger Zahlungsunwilligkeit des Käufers sind deshalb ein Betrug in Tateinheit mit Urkundenfälschung (§§ 263, 267, 52 StGB).

Dasselbe gilt beim Abschluss von Handy-Verträgen, wenn das Endgerät gleich ausgehändigt wird.

2.6.1.8 Einreichung gefälschter Schecks

Man sollte meinen, dass ein Kunde, der bei seiner Bank gefälschte Schecks zur Einziehung einreicht und dann den als Vorschuss gutgeschriebenen Scheckbetrag vom Konto abhebt, in böser Absicht handelt und betrügt. In einer neuen Entscheidung spricht sich der BGH für die Vermögensgefährdung aus, fragt aber auch danach, ob die Bank durch anderweitige Sicherheiten, zum Beispiel durch Kontoguthaben im Übrigen oder Zugriffsmöglichkeit auf andere Werte gesichert ist [223]:

---

[219] Jochen **Thielmann**, Andrea **Groß-Bölting**, Die "signifikante Erhöhung der Leistungswahrscheinlichkeit" als Vermögensschaden i.S.d. § 263 StGB, hrr-strafrecht.de Januar 2010.

[220] Dieter **Kochheim**, Skimming, März 2012 (Autorisierung)

[221] **BGH**, Beschluss vom 25.01.2012 - 1 StR 45/11, Rn 41.

[222] Unter Verweis auf: **BGH**, Urteil vom 22. August 2006 - 1 StR 547/05.

[223] **BGH**, Beschluss vom 06.03.2012 - 4 StR 669/11, Rn 9

Bei der betrügerischen Einreichung gefälschter Schecks trifft die über die Existenz einer wirksamen Scheckanweisung getäuschte Inkassobank durch die Erteilung der Vorbehaltsgutschrift eine Vermögensverfügung zu Lasten ihres Vermögens. Die Vorbehaltsgutschrift führt zu einer schadensgleichen Vermögensgefährdung, soweit der Kontoinhaber tatsächlich die Möglichkeit hat, auf den vorläufig gutgeschriebenen Scheckbetrag zuzugreifen (… [224]) und die Inkassobank nach den konkreten Umständen des Einzelfalles durch das ihr zukommende Rückbelastungsrecht nicht hinreichend gegen eine Vermögenseinbuße gesichert ist. Eine solche Sicherung der Bank ist in dem Umfang gegeben, in dem das Konto ohne Berücksichtigung der Vorbehaltsgutschrift ein Guthaben aufweist und zu erwarten steht, dass die Rückbelastung des Scheckbetrags wertmäßig abgedeckt sein wird. Aber auch in Fällen, in denen auf Grund der Rückbuchung mit einem Debetsaldo zu rechnen ist, fehlt es an einer schadensgleichen Vermögensgefährdung, soweit ein aus dem Wegfall der Vorbehaltsgutschrift resultierender Ausgleichsanspruch der Bank anderweitig, etwa durch das Pfandrecht der Bank aus Nr. 14 AGB-Banken, gesichert ist oder seitens der Bank ohne Schwierigkeiten realisiert werden kann, weil der Kontoinhaber zum Ausgleich des Kontos willens und in der Lage ist (… [225]).

2.6.1.9 Ergebnisse

Böse gesagt: Entscheidet sich der Bankkunde im laufenden Zahlungsdienstevertrag dazu, seine Bank zu schädigen, passiert ihm strafrechtlich nichts [226]. Nur wenn er seine Bank durch Lügen zur Einrichtung oder Erhöhung des Kreditrahmens veranlasst, seine Zahlungskarte missbräuchlich bei anderen Banken oder im Lastschriftverfahren einsetzt, macht er sich wegen Betruges (§ 263 StGB) oder wegen des Missbrauchs einer Scheckkarte strafbar (§ 266b StGB).

Auch der legendierte Bankkunde ist ein normaler Kontoberechtigter. Als solcher macht er sich bei der Kontoeröffnung wegen der Vorlage falscher Urkunden nur wegen Urkundenfälschung strafbar (§ 267 StGB). Erst wenn er neue Lügen bringt, um einen Überziehungskredit zu bekommen oder seinen Kreditrahmen ohne Zahlungswillen zu erhöhen, macht er sich wegen Betruges und bei der Verwendung falscher Urkunden strafbar.

Legt der Täter seinem Tatplan folgend falsche Urkunden sowohl bei der Kontoeröffnung als auch beim späteren Antrag auf einen Finanzierungskredit vor, dann handelt es sich um eine zwar mehraktige, aber einheitliche Tat Urkundenfälschung in Tateinheit mit Betrug (§§ 263, 267, 52 StGB).

Im Ergebnis gilt die 2001 vom BGH formulierte Konzeption fort: Spätestens mit der Übersendung der Zahlungskarte (und PIN) oder den Homebanking-Zugangsdaten verliert die Bank die Kontrolle über ihr Risiko. Damit ist der Kontoeröffnungsbetrug vollendet. Die automatisierten Verarbeitungsvorgänge im Zahlungsverkehr rechtfertigen es zudem, die Vollendung bereits zu dem Zeitpunkt anzunehmen, wann der Überziehungskredit in die EDV der Bank eingegeben wird [227].

---

[224] Verweis auf **BGH**, Beschluss vom 24. April 2007 – 4 StR 558/06.

[225] Im Original: *Vgl. zum Lastschriftbetrug BGH, Urteil vom 15. Juni 2005 – 2 StR 30/05 ... ; Beschluss vom 24. August 2005 – 5 StR 221/05 ... ; vom 14. September 2010 – 4 StR 422/10 ... ; a.A. OLG Hamm NJW 1977, 1834, 1836.*

[226] Siehe: Kontoeröffnung und Verfügungen unter einer Legende.

[227] Zu den besonders schweren Fällen im Vermögensstrafrecht siehe jetzt: CF, Vermögensverlust großen Ausmaßes und die Strafzumessung, 24.03.2012.

2.6.2 Handelsplattformen

Seit Jahren locken dubiose Anbieter auf allgemein zugänglichen Handelsplattformen und vermehrt in eigenen Webshops mit besonders günstigen Angeboten, in aller Regel mit Trendwaren aus dem Bereichen der Unterhaltungselektronik und der mobilen Telefonie. Dabei handelt es sich in vielen Fällen um nichts anderes als um Betrug (§ 263 StGB), weil es ihnen nur auf die Vorauszahlung des Kunden ankommt und die versprochene Lieferung nicht erfolgt. Andere Betrüger konzentrieren sich darauf, auf Handelsplattformen bekannter Anbieter (zum Beispiel eBay oder Amazon) Käufer mit begehrten Waren zu Geboten und schließlich zur Vorauszahlung oder zur Lieferung per Nachnahme zu locken. Dabei kommen auch alte Tricks wie das partnerschaftliche „Hochbieten“ zum Zuge, um geneigte Käufer zu höheren Geboten zu verlocken.

Bei einer förmlichen Versteigerung kommt zwischen dem Bieter und dem Auftraggeber ein Vertrag durch den Zuschlag des Versteigerers zustande (§ 156 BGB). Die Förmlichkeiten des Verfahrens regelt die Versteigerungsverordnung. Das besondere an der Versteigerung ist, dass die Mängelhaftung wegen des Versteigerungsgutes eingeschränkt ist (§ 445 BGB) und frühere Eigentumsrechte erlöschen (Pfand, Fund, Hinterlegung). Die förmlichen Voraussetzungen für Versteigerungen erfüllt zum Beispiel zoll.de, nicht aber die bekannten Handelsplattformen im Internet wie eBay und viele andere. Die hier angebotenen Waren und Dienste sind nach dem Recht der Auslobung zu behandeln, ein Vertrag kommt durch digitale Erklärungen und Einigung zustande [228] und die Versteigerungsverordnung findet keine Anwendung.

Der betrügerische Handel im Internet wird dadurch erleichtert, dass es relativ einfach ist, seine Identität zu verschleiern. Das beginnt bei der E-Mail-Adresse, die sich bei Massenanbietern mit beliebigen Personalien einrichten lässt. Phantasievolle Namen haben den Nachteil, dass sie als solche erkannt werden und Argwohn erregen. Mit ihnen lassen sich auch nur bedingt Bank- oder andere Verrechnungskonten oder Lieferadressen einrichten.

Deshalb sind die Zugangsdaten zu echten Kundendaten bei den Betrügern sehr beliebt (Identitätsdiebstahl). Sie sind auf dem Schwarzmarkt günstig zu haben und erzielen dann bessere Preise, wenn es sich um langlebige Konten handelt und deren Inhaber viele positive Bewertungen auf Handelsplattformen gesammelt haben [229]. Gehandelt wird alles, E-Mail-Adressen, Konten bei Versandhäuser, Handelsplattformen, Bankkonten und Zugangsrechte zu Packstationen. An die Zugangsdaten gelangen die Täter entweder durch reale Auftritte unter falschen Personalien, gezieltes Hacking oder durch das Ausspähen mit Malware.

Eine übliche Funktion der Malware ist es, den infiltrierten PC nach dem Einnisten nach persönlichen Daten zu untersuchen oder den Datenverkehr wegen der Kontozugangsdaten des Anwenders mitzuschneiden (Ausspähen und Abfangen von Daten, §§ 202a Abs. 1, 202b StGB) und an die Täter zu senden. Die Daten werden meistens auf „sicheren Speicherplätzen“ (Drops) gesammelt und häufig nach dem Vorbild von „Wundertüten“ unausgewertet als Ganzes verkauft oder zur Durchsicht anderen angeboten, die dann nur für die sie interessierenden Daten bezahlen. Soweit es sich dabei um *Passwörter oder sonstige Sicherungscodes* handelt, *die den Zugang zu Daten ... ermöglichen*, ist der Umgang mit ihnen strafbar (§ 202c Abs. 1 Nr. 1 StGB). Mit den so verschafften Daten lassen sich das fremde Konto aufrufen und die persönlichen Daten des Inhabers auslesen (§ 202a Abs. 1 StGB). Um den Inhaber von der Nutzung auszuschließen, verändern die Täter regelmäßig das Kennwort (§ 303b Abs. 1 Nr. 1 StGB), womit sie das Konto endgültig übernehmen und dem Datenbankserver ihre berechtigte Inhaberschaft vorspiegeln (§§ 269 Abs. 1, 270 StGB). Soll das Konto für Handelsgeschäfte verwendet werden, dann wer-

[228] **BGH**, Urteil vom 07.11.2001 - VIII ZR 13/01, Rn 14

[229] Vor allem aus englischsprachigen Carding-Boards ist bekannt, dass ganze Identitäten mit Lebenslauf, Personalpapieren, Bankkonto, Führerschein und Sozialversicherungsnummer gehandelt werden.

den in aller Regel die Wohnanschrift und die Daten zum Bankkonto zur Abwicklung des Zahlungsverkehrs verändert – wenn diese Daten nicht gleichzeitig gestohlen wurden [230]. Das so übernommene Konto lässt sich für alles mögliche missbrauchen, vor allem zum Betrug oder zum Computerbetrug (§§ 263, 263a StGB).

Das Tagesgeschäft eines Betrügers auf Handelsplattformen ist mühselig, weil er jeden Käufer zur Vorauszahlung oder zur Lieferung per Nachnahme überreden muss. Dann müssen die genervten Käufer mit schönen Geschichten hingehalten oder Päckchen für die Nachnahme-Käufer gepackt, mit nutzlosem Kram gefüllt und unter fremden Namen versandt werden. Auch die Warenbestellungen unter falschen Identitäten bedürfen logistischer Anstrengungen. Es müssen geneigte Empfänger für die Warensendungen gefunden (Hehlerei, § 259 StGB), Briefkästen mit vorgetäuschten Bewohnern eingerichtet oder Packstationen angemietet werden. Die dazu vorgetäuschten Identitäten sind schnell verbrannt und Bankkonten schnell gesperrt, so dass sie immer wieder durch neue ersetzt werden müssen. Das erfordert weitere (gefälschte) Personalpapiere, Post-Ident-Bescheinigungen oder Gehaltsnachweise [231].

2.6.3 Webshops

Mehr Beute versprechen öffentliche Webshops, in denen (nicht lieferbare) Waren zu günstigen Preisen und gegen Vorkasse angepriesen werden [232]. Auch ihre Lebensdauer ist begrenzt, weil die angeblichen Lieferschwierigkeiten und Hinhaltungen bald auffallen und sich in sozialen Netzwerken und speziellen Kommunikationsforen herumsprechen. Der Trick der Shopbetreiber hat mit dem „Stoßbetrug“ einen alten Namen. Dabei ging es ursprünglich darum, Lieferanten zu vermehrten Warenlieferungen auf Kredit zu veranlassen und die Waren auf Kasse, aber zu Spotpreisen abzusetzen. Die Lieferanten lassen sich darauf ein, weil sie gute Geschäfte wittern und viele Waren absetzen. Eine Variante davon wird häufig von den kriminellen Webshops gepflegt. Sie sagen Lieferungen gegen Vorkasse zu und setzen sich mit der Beute dann selber ab.

Ganz einfach ist der Betrieb eines kriminellen Webshops hingegen nicht. Der Betreiber muss eine Webseite einrichten, wozu einfache Werkzeuge zur Verfügung stehen, und sie im Internet präsentieren. Damit ist ihr Hostspeicherplatz lokalisierbar und setzt sich der Hostprovider peinlichen Fragen von Kunden, Rechtsanwälten und Strafverfolgern aus. Auch dagegen gibt es Spezialisten, die „Bullet-Proof“-Dienste anbieten und damit – in der Tradition des Russian Business Networks – werben, ihren Kunden Anonymität zu bieten und niemanden Auskunft über ihre Identität zu geben [233]. Sie betreiben Autonome Systeme – AS – als feste Bestandteile des Internets [234] und verschleiern den Standort der nötigen Server durch phantasievolle Meldungen der Geräte und bei den Whois-Antworten [235].

---

[230] PayPal und andere Anbieter haben Sicherheitsmechanismen eingebaut, die die Änderung der Stammdaten entweder verhindern oder dem Inhaber mitteilen. Ihre Umgehung wurde eindringlich in der Zeitschrift c't beschrieben:
CF, Betrug mit PayPal, 12.09.2010; Axel Kossel, Verkäufer ohne Schutz, c't 20/2010, S. 76 .

[231] Wegen der Rechtsprobleme bei Urkundenfälschungen (§ 267 StGB) im Zusammenhang mit Kopien, Faxen und digitalen Abbildungen siehe ▸ Urkunde und Abbild.

[232] Das LKA Bayern hat im Mai 2011 acht Leute festgenommen, die mit betrügerischen Webshops 100.000 Menschen um mehrere Millionen Euro geprellt haben sollen: Betrug im Internet: Polizei hebt Bande aus, Heise online 17.05.2011.

[233] Die Rede ist von Schurkenprovidern: Dieter **Kochheim**, Cybercrime, 24.05.2010, S. 80.

[234] Dieter **Kochheim**, Netzkommunikation, 10.07.2010, S. 17 (Geroutete Welt).

[235] Whois Protection und Anonyme Server, siehe:

Neuere Erscheinungsformen arbeitsteiliger Tätergruppen pflegen intensive Kommunikationsbeziehungen innerhalb einer abgrenzbaren Gruppe, deren Beteiligte nach Maßgabe eines Grundkonsenses handeln: Keiner muss zur Begehung von Straftaten überredet werden, sie sind durchweg tatgeneigt und zur kriminellen Zusammenarbeit in wechselnden Konstellationen bereit. Dabei binden sie sich in aller Regel nicht über den einzelnen Vorgang hinaus, bleiben aber kontinuierlich in Kontakt zueinander und finden sich immer wieder zur gemeinsamen Begehung verschiedener Taten zusammen. Sie verbindet miteinander, dass sie einen Beuteanteil aus dem einzelnen „Geschäft" erzielen oder durch ihre Beteiligung bereits bestehende Schulden getilgt haben wollen. Der Grundkonsens ist leitend für die Tatausführung im Einzelnen.

Jedenfalls dann, wenn die Schwarmtäter mindestens zweimal gemeinsame Taten ausführen, muss davon ausgegangen werden, dass sie von dem beschriebenen Grundkonsens motiviert sind und bandenmäßig handeln. Das ist der Fall, wenn

- *die Tätergruppe eingrenzbar ist und intensive Kommunikationsbeziehungen pflegt,*
- *die Beteiligten tatgeneigt sind, so dass sie im Einzelfall nicht zur Beteiligung an Straftaten überredet werden müssen,*
- *mindestens drei Täter wiederholt und in wechselnder Zusammensetzung bei der Tatplanung oder -ausführung zusammen arbeiten und*
- *die Zusammenarbeit Delikte der gleichen Art betreffen.*

CF, kommunizierende Schwärme und zugeneigte Banden, 01.07.2010

Damit ist es nicht getan. Der Webshop-Betreiber muss seine Kommunikation per E-Mail oder anderen Diensten tarnen und den Zahlungsverkehr gegen Rückbuchungen sichern [236]. Dafür gibt es Webmailer und vorgebuchte Adressen, Anonymisierer und schließlich Spezialisten für das Inkasso und die Geldwäsche, die aber alle mitverdienen wollen.

Webshops kommen auch in einer nichtöffentlichen Variante vor. Die Betreiber geschlossener Boards verkaufen gelegentlich Monopollizenzen, die dem Mitglied den exklusiven Handel gegegneine monatliche Miete [237] mit bestimmten Waren und Diensten garantiert, zum Beispiel mit Skimming-Geräten, Onlinebanking-Trojanern, Trojaner-Baukästen und sogar Waffen oder Rauschgift [238]. Nach der erfolgreichen Polizeiaktion gegen das Elite-Forum [239] schienen sie zunächst verschwunden zu sein [240], sind jetzt aber wieder da. Das Publikum ist zwar auf die Mitglieder des Boards begrenzt, aber exklusiv und geneigt. Die Abschottung nach außen und die sichere Zahlungsabwicklung durch Treuhandaufträge [241] besorgt der Boardbetreiber, der an allen Geschäften verdient.

Die Erfahrungen mit den sozialen Beziehungen einerseits zwischen den Schurkenprovidern und ihren Kunden sowie andererseits zwischen Bord-Administratoren und ihren Mitgliedern sind noch gering.

Über die weitläufigen kriminellen Strukturen im Bereich der Cybercrime mit einem Schwerpunkt bei den Tätern mit russischsprachiger Herkunft hat vor allem Paget berichtet [242]. Seine Materialfülle ist

Dieter **Kochheim**, Cybercrime, 24.05.2010, S. 114, 115.

[236] Am besten per WebMoney, denn hier gilt das eiserne (russische) Prinzip, dass keine Verfügung wieder rückgängig gemacht wird.

[237] Marc-Aurél **Ester**, Ralf **Benzmüller**, G Data Whitepaper 2009. Underground Economy, 19.08.2009, S. 5 f.

[238] Ebenda, S. 4.

[239] Dieter **Kochheim**, Cybercrime, 24.05.2010, S. 103 (Basar für tatgeneigte Täter)

[240] Marc-Aurél **Ester**, Ralf **Benzmüller**, Whitepaper 04/2010. Underground Economy - Update 04/2010, G Data 22.04.2010, S. 2, 3, 8.

[241] Um sich gegen die Betrügereien im eigenen Umfeld zu wappnen, bieten die Moderatoren und Administratoren in Carding-Boards Treuhanddienste an, die wie die Verwaltung von Anderkonten von Notaren und Rechtsanwälten funktionieren. Erst wenn die Zahlung des Käufers bei ihm eingegangen ist, gibt der Treuhänder die Warenlieferung frei. Nach Abzug seiner gerechten Gebühr zahlt der Treuhänder den Händler aus, sobald der Käufer den Empfang der Leistung mitgeteilt hat. Gelegentlich wirtschaftet der Treuhänder in die eigene Tasche und wird dann als Scammer (Betrüger) gebannt und womöglich auch bedroht.
Siehe auch: François **Paget**, Cybercrime and Hacktivism, McAfee 15.03.2010, S. 55.

[242] Dieter **Kochheim**, Cybercrime und politisch motiviertes Hacking. Über ein Whitepaper von

> *Das ... Geschäftsmodell des RBN war simpel und dreist: Je mehr eine Domain in den Fokus der Öffentlichkeit geriet, je mehr Beschwerden an die EMail-Adresse für Missbrauch geschickt wurden, desto mehr Geld verlangten die Russen von ihren Kunden.*
>
> Gordon Bolduan, Digitaler Untergrund, Technology Review 4/2008, S. 32

bemerkenswert. Was ihm fehlt, ist der kriminalistisch geschulte Blick auf Personenzusammenhänge und soziale Beziehungen. So ist ihm zum Beispiel entgangen, dass CarderPlanet [243] eine innere Struktur in der Tradition der „Diebe im Gesetz“ [244] aufweist und dass sich die Beziehungen und Gruppenidentitäten in der russischen Sprachkultur besonders auf Kommunikation und darauf fußen, wer mit wem spricht und wer wen unterstützt. Dadurch entsteht eine komplizierte soziale Struktur, die zwar Hierarchien aufweist, die aber weniger der Herrschaftsausübung als dem Interessenausgleich zwischen den beteiligten Gruppen dient [245]. Ich habe das 2010 als ein schwarmähnliches Verhalten beschrieben, das auf intensiven Kommunikationsbeziehungen innerhalb abgrenzbarer, aber offener Gruppen tatgeneigter Beteiligter beruht [246].

Das Russian Business Network – RBN – aus St. Petersburg wurde von mehreren Autoren beschrieben [247] und am eindringlichsten wohl von Faber [248]. Sie zeigen vor allem die enge technische Einbindung der betriebenen Infrastruktur für Schurkenprovider und die soziale Integration der Betreiber, die vom Wohlwollen und der Duldung ihres sozialen Umfeldes und der staatlichen Einrichtungen abhängen. Die auslösenden Gründe für das Abtauchen des RBN sind bis heute unbekannt geblieben.

Tiefe Einblicke in die – vor allem deutschen – Board-Kulturen und -Strukturen vermitteln Ester und Benzmüller [249]. Sie beschränken sich auf Beobachtungen in geschlossenen Benutzerkreisen und berichten deshalb nur über die Kommunikation, die andere Beteiligte im Bereich der Carding-Szene führen. Bereits daraus lässt sich ableiten, dass mehrere Personenrollen aus dem Kreis der Mitglieder herausragen.

- Die Administratoren sind die Betreiber der Boards. Sie richten es ein und betreiben den technischen Rahmen des Boards, bestimmen über die Zulassung neuer Mitglieder und gewähren den bewährten Mitgliedern und Moderatoren zunehmende Zugriffs- und Gestaltungsrechte. Neue Mitglieder müssen sich gelegentlich ausdrücklich bewerben, ihre kriminellen Leistungen und Erfahrungen beschreiben oder werden nur auf Empfehlung oder Zuspruch von Bürgen zugelassen. Die Administratoren verdienen an den Zulassungsgebühren, den obligatorischen Treuhandgeschäften und den Gebühren, die exklusive Webshopbetreiber bezahlen müssen.

- Die Moderatoren betreuen einzelne Threats (Themenkreise), stellen Beziehungen und Verbindungen zwischen den Mitgliedern her und sind wegen ihrer Vertrauensstellung von der Treuhandbindung wegen eigener Geschäfte befreit. Auch zwischen den Moderatoren kann es Abstufungen geben (First, Second, Third Level), in deren Rahmen sie bei besonderem Wohlverhalten aufsteigen können. Auch sie verdienen an den Treuhandgebühren im Zusammenhang mit den von ihnen betreuten Threats und gelegentlich wohl auch an Beuteanteilen.

- Die Webshopinhaber zahlen für ein Handelsmonopol. Das lohnt sich nur, wenn sie erheblichen

François Paget von den McAfee Labs, 20.10.2010; François **Paget**, Cybercrime and Hacktivism, McAfee Labs 15.03.2010.

[243] Paget, S. 6

[244] **CF**, Geschichte und Fraktionen der Mafia, 14.06.2011; Diebe im Gesetz, kripo.at 28.08.2011.

[245] Diese Erkenntnis leitet der BND aus öffentlichen Quellen ab.

[246] **CF**, kommunizierende Schwärme und zugeneigte Banden, 01.07.2010

[247] Siehe die Nachweise bei: **CF**, Russian Business Network – RBN, 13.07.2008.

[248] Frank Faber, Unter Verdacht. Eine russische Bande professionalisiert das Cybercrime-Business, c't 11/2008

[249] Marc-Aurél **Ester**, Ralf **Benzmüller**, Underground Economy, G Data Whitepaper 2009, 19.08.2009

Profit durch ihre Geschäfte erwarten.

Dieses Rollenmodell ist aus verschiedenen Berichten abgeleitet und keineswegs als gesicherte Erkenntnis zu behandeln, zumal die Geflogenheiten von Board zu Board wechseln und auch selber im Fluss sein dürften. Es erklärt die monetären Beweggründe, ein Board einzurichten und sich an seiner aktiven Gestaltung zu beteiligen, nicht aber die Prozesse, die zur Bildung von Subkulturen im Internet und dazu geführt haben, dass sie sich jedenfalls teilweise von gesellschaftlichen Moralvorstellungen abgelöst und offen kriminelle Geschäfte tätigen. Ein Grund dafür dürfte die relative Sicherheit sein, in der sie agieren und erwarten, nicht strafverfolgt zu werden. Hinzu dürfte ein abgegrenztes, subkulturelles Selbstverständnis kommen, das sich in eigenen Sprachgewohnheiten und Kommunikationsprozessen äußert (siehe auch: ▸ Selbstverständnis der Täter).

2.6.4 Abofallen

Warnecke und Knabe, zwei führende Polizeibeamte aus Göttingen, berichteten in der Zeitschrift Kriminalistik [250] über zwei Umfangsverfahren im Zusammenhang mit Abofallen und der Entfernung von SIM-Lock-Sperren [251]. Wegen der Abofallen geben sie Anlass zu interessanten Rechtsfragen und einen Einblick in die besondere Gedankenwelt der Täter.

Der beschriebene Fall geht auf das Jahr 2007 zurück [252]: Die drei jungen Täter *hatten im Jahre 2007 unter der Domain fabrik-einkauf.com ihre Abofalle ins Leben gerufen. Per Spam bewarben sie die Seite sowie ein angebliches Gewinnspiel. Wer dort seine Daten hinterließ um Zugang zu erhalten, erhielt wie bei der Masche üblich eine Aborechnung (84 Euro/Jahr)*.

2.6.4.1 klassische Abofalle

Das übliche Vorgehen ist gewesen, mit dem besonders schnellen Download freier Open Source-Software oder Shareware [253] zu werben. Mit diesem Versprechen wurden die Kunden auf Webseiten gelockt und zur Eingabe einiger persönlicher Angaben überredet. Die Tatsache, dass mit dem abschließenden „Abschicken“ ein (meistens) zweijähriger Abovertrag abgeschlossen wurde, wurde irgendwo auf der Webseite mit möglichst kleinem und unauffälligem Text versteckt. Dieser Trick erinnert an den klassischen Offertenbetrug [254], dem der BGH im Jahr 2001 ein klares Ende gesetzt hat

---

250 Volker **Warnecke**, Oliver **Knabe**, Abofallen und Simlockentfernung. Ermittlungstaktische Erfahrungen und rechtliche Bewertung spezieller Formen der IuK-Kriminalität, Kriminalistik 7/2011, S. 448 (kostenpflichtige Vollversion)

251 **CF**, SIM-Lock-Hacking, 23.10.2010

252 Abofallen-Betreiber zu Haftstrafen verurteilt, Heise online 17.08.2009

253 Shareware: Kommerzielle Software, deren Nutzung vorübergehend (zur Probe) kostenfrei ist und die frei verbreitet werden darf. Beispiel: Anklage wegen Abzocke mit Abofallen, Heise online 23.10.2011

254 **CF**, Offertenbetrug, 02.08.2008

[255]: *Wer Angebotsschreiben planmäßig durch Verwendung typischer Rechnungsmerkmale (insbesondere durch die hervorgehobene Angabe einer Zahlungsfrist) so abfasst, dass der Eindruck einer Zahlungspflicht entsteht, dem gegenüber die - kleingedruckten - Hinweise auf den Angebotscharakter völlig in den Hintergrund treten, begeht eine (versuchte) Täuschung im Sinne des § 263 Abs. 1 StGB.* Das gilt auch für den beschriebenen Abofallen-Trick, wie 2010 das OLG Frankfurt a.M. entschieden hat [256]: *Hiernach ist die Täuschung jedes Verhalten, das objektiv irreführt oder einen Irrtum unterhält und damit auf die Vorstellung eines anderen einwirkt. Dabei kann die Täuschung außer durch bewusst unwahre Behauptungen auch konkludent durch irreführendes Verhalten, das nach der Verkehrsanschauung als stillschweigende Erklärung zu verstehen ist, erfolgen. Davon ist auszugehen, wenn der Täter die Unwahrheit zwar nicht expressis verbis zum Ausdruck bringt, sie aber nach der Verkehrsanschauung durch sein Verhalten miterklärt.*

Es liegt nahe, dass es sich bei der Anmeldeprozedur und dem anschließenden Inkasso um einen automatisierten Vorgang handelt, so dass auf ihn die Grundsätze anzuwenden sind, die auch für die Verbreitung von Bot- und Malware gelten und im Zusammenhang mit dem ▸ Rückruftrick entwickelt wurden: Der Täter handelt nur einmal, so dass sich aus seiner Sicht alle Einzelfälle als Teilakte einer einheitlich Tat darstellen.

Der Betrug stellt jedoch höhere Anforderungen an die Handlungen der Beteiligten und fordert, dass der Täter zunächst über eine Tatsache täuscht, das Opfer darauf einem Irrtum unterliegt und deshalb eine Vermögensverfügung trifft, die beim Täter stoffgleich zu einem Vermögensgewinn führt.

Bei der klassischen Abofalle [257] erfolgen jedoch zwei Täuschungshandlungen. Zunächst ist das die Täuschung über den Abschluss eines kostenträchtigen Vertrages, die den Beginn des Versuches einleitet (§ 22 StGB). Hinzu kommt die konkrete Aufforderung [258], zu zahlen, weil (angeblich) ein bindender Vertrag abgeschlossen wurde. Die erstrebte Vermögensverfügung erfolgt erst anschließend, wenn der eingeschüchterte „Kunde“ auch tatsächlich bezahlt. Erst mit dem Zugang des Geldes ist der Betrug vollendet. Das damit verbundene Handlungsmodell erfordert aber mindestens zwei Handlungen des Täters: Die automatisierte Übertölpelung des Webseitenbesuchers und die bewusste Entscheidung, ihn anschließend mit überraschenden Forderungen zu überziehen und dazu individualisierte Briefe zu generieren, zu adressieren und schließlich auf den Postweg zu geben – was sich nicht mehr als einheitlicher automatisierter Vorgang darstellt.

Zu fragen ist deshalb, ob nicht doch schon in dem unüberlegten „Klick“ des Webseitenbesuchers eine Vermögensverfügung versteckt ist, die den Betrug zur Vollendung bringt. Das legt jedenfalls die über lange Jahre entwickelte Rechtsprechung zur schadensgleichen Vermögensgefährdung nahe, durch die *eine Gefahrensituation eine solche Intensität erreicht hat, dass sie einer endgültigen Vermögenseinbuße gleichgestellt werden kann* [259]. Das ist nur dann der Fall, wenn eine *vom Berechtigten nicht mehr zu kontrollierende und nur noch im Belieben des Täters stehende Möglichkeit des endgültigen Vermögensverlustes besteht* [260]. 2010 hat das BVerfG schließlich gefordert [261], *die Schadensfeststellung auf eine sichere Grundlage zu stellen, sie rational nachvollziehbar zu machen und sich zu vergewissern, ob im Einzelfall eine hinreichend sichere Grundlage für die Feststellung eines Vermögensnachteils*

---

[255] **BGH**, Urteil vom 26.04.2001 – 4 StR 439/00, Leitsatz

[256] **OLG Frankfurt a.M.**, Beschluss vom 17.12.2010 – 1 Ws 29/09, Rn 32

[257] Anschauliches Beispiel: Neue Masche im Internet - Wenn „kostenlos“ 84 Euro kostet, c't-TV 11.06.2011.

[258] Mit markigen Worten, siehe zum Beispiel: Von App-Zocke bis Zwangsabo, c't-TV 20.10.2010.

[259] **BVerfG**, Beschluss vom 10.03.2009 - 2 BvR 1980/07, Leitsatz 6

[260] **BVerfG** ebenda.

[261] **BVerfG**, Beschluss vom 23.06.2010 - 2 BvR 2559/08, 105/09, 491/09; wegen der Einzelheiten: **CF**, BVerfG: Bezifferter Gefährdungsschaden, 15.08.2010

überhaupt existiert oder ob man sich in einem Bereich bewegt, in dem von einem zahlenmäßig fassbaren Schaden noch nicht die Rede sein kann. Soweit Unsicherheiten verbleiben, ist unter Beachtung des Zweifelssatzes der (Mindest-) Schaden im Wege der Schätzung zu ermitteln ...

Seit seiner Entscheidung vom Februar 2009 sieht jedenfalls der 1. Strafsenat des BGH die schadensgleiche Vermögensverfügung als entbehrlich an [262], wenn mit betriebswirtschaftlichen und kaufmännischen Mitteln überhaupt ein Schaden beziffert werden kann, der sich auch am Verlustrisiko orientieren darf. Das ist aber nur der Fall, wenn der Geschädigte eine Vermögensverfügung trifft und dafür im Gegenzug keine werthaltige Gegenleistung erwarten kann. Diese Linie wurde vom 3. Strafsenat des BGH aufgenommen und auf wegen der Rückzahlung wertloser Darlehnsverträge [263] sowie auf Versicherungsverträge angewendet, die nur in der Absicht abgeschlossen wurden, die Versicherung mit fingierten Schadensfällen zu betrügen [264], weil eine signifikante Erhöhung des vertraglichen Einstandsrisikos bestehe [265].

Auf die klassische Abofalle angewendet führt diese Rechtsprechung eher dazu, in dem einfachen „Klick“ noch keine bezifferbare Vermögensgefahr zu sehen. Der Webseitenbesucher gibt zwar durch tatsächliches Handeln eine rechtsgeschäftliche Erklärung ab, verbindet das aber nicht mit einer Vermögensverfügung. Die könnte in dem durch Täuschung entstehenden Abwehrrisiko gesehen werden. Dem ist jedoch entgegen zu halten, dass die Abofallenbetreiber und die von ihnen mit dem Inkasso betrauten Anwälte zwar erfahrungsgemäß markige Mahnungen von sich gegeben, im Zweifel aber das Prozessrisiko gemieden haben.

2010 hat der 3. Strafsenat seine Rechtsprechung präzisiert und der Vermögensgefährdung den Eingehungsschaden entgegen gestellt [266]. Er unterscheidet zwischen:

- Dem ***Eingehungsschaden***, der sich aus der rechnerischen *Gegenüberstellung der wirtschaftlichen Werte der gegenseitigen vertraglichen Ansprüche* beim Vertragsabschluss selber ergibt [267]. Gemeint ist der Vergleich der wirtschaftlichen Werte der beiderseitigen Vertragspflichten nach einer noch abstrakten Berechnung.

- Dem ***Erfüllungsschaden*** als materialisierter Schaden. Er realisiert sich durch die *Erbringung der versprochenen Leistung des Tatopfers ... und bemisst sich nach deren vollen wirtschaftlichen Wert, wenn die Gegenleistung völlig ausbleibt* [268]. Gemeint sind die unmittelbaren Verfügungen, die aufgrund des Vertragsabschlusses erfolgen (Gegenstand der Übereignung, Provision als solche). Ihm sind die Gegenleistungen des Täters (Anzahlung, Kaution, Nachnahme) gegenzurechnen.

- Die ***weitergehenden Vermögensnachteile***, *die der Geschädigte aufgrund der irrtumsbedingten Vermögensverfügung erleidet* [269], ohne dass der Täter seinem Plan entsprechend einen spiegelbildlichen Vermögensvorteil erlangt. Dieser nicht der Stoffgleichheit unterliegenden Schaden ist vorher unter dem Begriff "Folgeschaden" diskutiert worden.

An der Beurteilung der klassischen Abofalle ändert sich dadurch nichts. Bei ihr fallen bewertbare Eingehungs- und Erfüllungsschäden erst an, sobald der Webseitenbesucher eingeschüchtert bezahlt. Alle anderen Handlungen sind noch im Versuchsstadium angesiedelt. Auslöser dafür ist das erste Forderungsschreiben. Werden gleichzeitig mehre-

---

[262] **BGH**, Beschluss vom 18.02.2009 - 1 StR 731/08; wegen der Einzelheiten: **CF**, Beeinträchtigung und Verlust, 13.1.2010.

[263] **BGH**, Urteil vom 13.08.2009 - 3 StR 576/08

[264] **BGH**, Urteil vom 14.08.2009 - 3 StR 552/08

[265] Diesen Teil der Entscheidung hat das BVerfG als tatbestandsausweitende Überdehnung der Strafbarkeit kassiert: **BVerfG**, Beschluss vom 07.11.2011 - 2 BvR 2500/09, 1857/10, Rn 162 ff.

[266] **BGH**, Beschluss vom 07.1.2010 - 3 StR 433/10; vom Gegenstand her identisch mit **BGH**, Beschluss vom 07.1.2010 - 3 StR 434/10; wegen der Einzelheiten: **CF**, Der Eingehungsschaden löst den Gefährdungsschaden ab, 16.02.2011.

[267] **BGH** ebenda, Rn 10.

[268] **BGH** ebenda, Rn 10.

[269] **BGH** ebenda, Rn 12.

re oder viele Forderungsschreiben verfasst und versandt, dürfte seitens der Täter zwar keine natürliche Handlungseinheit vorliegen, wohl aber eine von einem einheitlichen Handlungsvorsatz getragene deliktische Einheit [270].

2.6.4.2 Göttinger Abofalle

Die drei Angeklagten aus Göttingen sind zu verhaltenen Freiheitsstrafen verurteilt worden, deren Vollstreckungen zur Bewährung ausgesetzt wurden [271]. Ihr Vorgehen weicht stark von der klassischen Abofalle ab.

Zwischen dem 31.08. und dem 15.10.2007 starteten sie insgesamt zehn Spam-Kampagnen, mit denen sie in fast 1.000 Fällen erfolgreich zum Aufruf von präparierten Webseiten verlockten. Die persönlichen Daten der Empfänger entnahmen sie einer 600.000 Personaldaten umfassenden Datensammlung eines Frankfurter Unternehmens, die sie sich unberechtigt beschafft hatten. Die URLs [272] zu den präparierten Webseiten enthielten eine individuelle Personalisierungsnummer, die dort zusammen mit der angelieferten IP-Adresse ausgelesen und in eine Datenbank geschrieben wurden. So verfuhren sie mit allen Geschädigten (siehe wegen der weiteren Einzelheiten den Kasten rechts). Unter Verbindung mit den Personendaten aus der schon vorhandenen Datensammlung schrieben die Täter alle Geschädigten an, behaupteten, sie hätten ihre Personaldaten selber eingegeben, einer kostenpflichtigen Mitglied zugestimmt und forderten 86 € Mitgliedschaftsgebühr. Damit sollen die Täter mehr als 130.000 € als Beute erlangt haben.

Das Landgericht Göttingen legt seinem Urteil zehn Taten des Betruges zugrunde (§ 263 StGB), wobei es die verschiedenen Taten an den einzelnen Spam-Aktionen festmacht [273]. Einen der drei Täter betrachtet es nicht als Mittäter, sondern als Gehilfen (§§ 25 Abs. 2, 27 Abs. 1 StGB), so dass die Täter keine Bande bilden konnten [274].

Das abgekürzte Urteil, das nicht vollständig veröffentlicht ist, lässt die Auseinandersetzung mit zwei Fragen vermissen, die nach der Gewerbsmäßigkeit des Täterhandelns und nach der Bedeutung der vorab beschafften Kundendaten, die für die Personifizierung der Spam-Mails genutzt wurden.

Nach den Meldungen in der Presse sind die Göttinger Täter wegen gewerbsmäßigen Betruges verurteilt worden [275] und das macht den „normalen“ Betrug zu einem besonders schweren Fall (§ 263 Abs. 3 Nr. 1 StGB) mit einer Strafdrohung von sechs Monaten bis zu zehn Jahren Freiheitsstrafe. Im Strafausspruch wird nur der Grundtatbestand genannt und nicht auch, dass es sich um einen besonders schweren Fall handelt (Arg. aus § 12 Abs. 3 StGB).

Die Frage nach der Kundendatenbank, die für die Tat verwendet wurde, veranlasst mich zu folgenden Überlegungen:

Allein das sich Verschaffen und die Nutzung einer unberechtigt erlangten Kundendatenbank dürfte als eigennütziges Verschaffen und Verwertung fremder Geschäftsgeheimnisse im Sinne von § 17 Abs. 2 Nr. 1. und 2. UWG anzusehen sein, wofür drei Jahre Freiheitsstrafe drohen. Das Tatbestandsmerkmal „Eigennutz“ steht selbständig und ist nicht an die besonderen Merkmale „Wettbewerb“ oder „Schaden zufügen“ gebunden,

---

[270] Grundlagen und Einzelheiten: Dieter **Kochheim**, Skimming, 22.04.2011, S. 21 (natürliche Handlungseinheiten).

[271] **LG Göttingen**, Urteil vom 17.08.2009 - 8 Kls 1/09

[272] URL, umgangssprachlich „Link“. Wegen der Adresszusätze und Manipulationsmöglichkeiten siehe: Dieter **Kochheim**, Cybercrime, 24.06.2010, S. 32 (Adressierung im Internetprotokoll).

[273] Tatmehrheit beim Bandenbetrug: **BGH**, Beschluss vom 29.07.2009 - 2 StR 160/09.

[274] Die Bildung einer Bande setzt mindestens 3 Täter voraus, die sich an ihr als Mittäter beteiligen wollen: **Großer Senat des BGH**, Beschluss vom 22.03.2001 - GSSt 1/00.
Mittäterschaft: **BGH**, Beschluss vom 07.1.2010 - 3 StR 433/10; Beihilfe: **BGH**, Beschluss vom 23.12.2009 - 1 BJs 26/77-5 - StB 51/09;
Verabredung zu einem Verbrechen: **BGH**, Beschluss vom 14.04.2011 - 1 StR 458/10.

[275] Abofallen-Betreiber zu Haftstrafen verurteilt, Heise online 17.08.2009

Im Text der Email wurde den Adressaten wahrheitswidrig eine geheime Liste mit Adressen von Großhändlern sowie Tipps, wie man bei diesen zu Großhandelspreisen Elektrogeräte erwerben könnte, in Aussicht gestellt. Zudem wurden einige Beispielangebote genannt. Gleichzeitig wurde darauf hingewiesen, dass der Absender selber keine Produkte verkaufen wolle.

Die Emails enthielten drei Links zu einer sog. Sprungbrettseite. Jeder Link enthielt am Ende eine fünf- bis siebenstellige Personalisierungsnummer, die eine Zuordnung zu dem jeweiligen Adressaten ermöglichte. Wenn also ein Adressat auf den Link klickte, wurde ohne seine Kenntnis mit Hilfe sog. PHP-Skripten automatisch eine Verbindung zwischen ihm und seinen vollen Personaldaten aus der auf dem Server befindlichen Datenbank hergestellt. So war eine Personalisierung der weiteren Schreiben möglich, ohne dass der Betreffende seine persönlichen Daten irgendwo eingeben hätte.

Auf der jeweiligen Sprungbrettseite befand sich ein Button mit der Aufschrift "Direkt zum Fabrikeinkauf", der auf die Seite "R" verlinkte. Zudem wurde das Angebot ähnlich wie in der Email beworben. Nur im unteren Bereich der Seite, der ohne Herunterscrollen nicht sichtbar war, befand sich in kleiner Schrift folgender Hinweis: "Für den Zugriff auf den Mitgliederbereich zahlen Sie einmalig 86 €. …“

LG Göttingen, Urteil vom 17.08.2009 - 8 Kls 1/09

so dass allein die Tatsache der Nutznießung zur tatbestandlichen Erfüllung ausreichen dürfte.

Die Einbindung der Daten in eine neue Datenbank und die präparierte Webserverumgebung macht die Tat zum Dauerdelikt im Hinblick auf die zehn aufeinander folgenden Spam-Kapagnen, so dass es sich um einen gewerbsmäßigen und besonders schweren Fall mit einer erhöhten Strafdrohung von fünf Jahren Freiheitsstrafe handeln dürfte (§ 17 Abs. 3 UWG).

Dauerdelikte wie die gewerbsmäßige Verwertung von Geschäftsgeheimnissen können eine materielle Klammerwirkung jedenfalls auf solche Delikte ausbilden, die mit ihm in enger Verbindung stehen [276]. Das würde auch für die Spam-Kapagnen gelten, die dem Landgericht Göttingen die Grundlage für zehn Einzeltaten des Betruges gegeben haben.

Das ist nicht in jedem Fall so: *Denn eine minder schwere Dauerstraftat hat nicht die Kraft, mehrere schwerere Einzeltaten, mit denen sie ihrerseits jeweils tateinheitlich zusammentrifft, zu einer Tat im Sinne des § 52 Abs. 1 StGB zusammenzufassen ...* [277]. So ist es grundsätzlich ausgeschlossen, dass ein Vergehen mehrere Verbrechen zu einer Tat zu verklammert (bei der kriminellen Vereinigung): *Das ist bei den Verbrechen, die Gegenstand dieses Strafverfahrens sind und für die das Gesetz erheblich höhere Strafen androht als § 129 StGB, nicht der Fall. Diese Straftaten stehen deshalb zu den bereits abgeurteilten, ebenfalls in Tateinheit zu § 129 StGB stehenden Vergehen in Realkonkurrenz* [278].

Würde es sich bei den zehn Taten der Göttinger Abofallen-Täter um "einfache" Betruge im Sinne von § 263 Abs. 1 StGB handeln, dann würde das gewerbsmäßige UWG-Vergehen eine solche Klammerwirkung entfalten, weil sie mit derselben Höchstfreiheitsstrafe von fünf Jahren drohen. Das hätte zur Folge gehabt, dass die Täter nur wegen einer materiellen Straftat des sich Verschaffens und der Verwertung fremder Geschäftsgeheimnisse in Tateinheit mit Betrug mit einer Höchstfreiheitsstrafe von fünf Jahren hätten verurteilt werden können.

Der gewerbsmäßige Betrug (§ 263 Abs. 3 Nr. 1 StGB) droht hingegen mit zehn Jahren Freiheitsstrafe im Einzelfall und würde damit die Klammer sprengen. Das gilt auch für den gewerbsmäßigen Bandenbetrug (§ 263 Abs. 5 StGB). Er ist ein selbständiger Verbrechenstatbestand, droht mit Freiheitsstrafe von einem bis zu zehn Jahren und sprengt die Klammer vom UWG-Vergehen ebenfalls.

---

[276] **BGH**, Beschluss vom 19.04.2011 – 3 StR 230/10, Rn 15 bis 17 (kriminelle Vereinigung);
BGH, Beschluss vom 02.12.2008 - 3 StR 203/08, Rn 17 (Strafvereitelung, gemeinsamer Vereitelungswille wegen mehrerer Verunglimpfungen, Beleidigungen und Nötigungen).

[277] **BGH**, Beschluss vom 10.11.2010 - 5 StR 464/10, Rn 3

[278] **BGH**, Urteil vom 11.06.1980 - 3 StR 9/80, Rn 8

Gewerbsmäßig handelt, wer sich durch wiederholte Tatbegehung eine nicht nur vorübergehende Einnahmequelle von einigem Umfang und einiger Dauer verschaffen will. Liegt diese Absicht vor, ist bereits die erste Tat als gewerbsmäßig begangen einzustufen, auch wenn es entgegen den ursprünglichen Intentionen des Täters zu weiteren Taten nicht kommt. Eine Verurteilung wegen gewerbsmäßiger Deliktsbegehung setzt daher schon im Grundsatz nicht notwendig voraus, dass der Täter zur Gewinnerzielung mehrere selbstständige Einzeltaten der jeweils in Rede stehenden Art verwirklicht hat. Ob der Angeklagte gewerbsmäßig gehandelt hat, beurteilt sich vielmehr nach seinen ursprünglichen Planungen sowie seinem tatsächlichen, strafrechtlich relevanten Verhalten über den gesamten ihm anzulastenden Tatzeitraum (...). Erforderlich ist dabei stets, dass sich seine Wiederholungsabsicht auf dasjenige Delikt bezieht, dessen Tatbestand durch das Merkmal der Gewerbsmäßigkeit qualifiziert ist.

BGH, Beschluss vom 01.09.2009 - 3 StR 601/08, Rn 5

Diese akademisch anmutenden Erwägungen zeigen, dass ganz kleine Weichenstellungen im Zusammenhang mit der materiellrechtlichen Bewertung von Sachverhalten zu stark voneinander abweichenden Strafrahmen führen können. Angewandt auf die Göttinger Abofalle:

- Der Grundtatbestand der Ausführungstaten ist der Betrug (§ 263 Abs. 1 StGB), der als mittelschweres Vergehen mit einer Höchstfreiheitsstrafe von fünf Jahren droht.

- Die Handlungsserie ist von zehn Handlungsentscheidungen geprägt, die sich an den durchgeführten Spam-Kapagnen festmachen lassen. Sie führen zu einer Tatmehrheit (§ 53 StGB) von zehn Betrugen, die zu einer Gesamtfreiheitsstrafe verbunden werden müssen, deren Höhe auf fünfzehn Jahre Freiheitsstrafe begrenzt ist (§ 54 Abs. 2 S. 2 StGB).

- Zwei der Täter handelten als Mittäter (§ 25 Abs. 2 StGB) und müssen für die Tathandlungen des jeweils anderen einstehen. Der dritte Täter unterstützte die anderen als Gehilfe (§ 27 StGB) dadurch, dass *er das in der Rechnung angegebene Konto eröffnete und verwaltete, die eingegangenen Gelder weiterverfügte, erforderliches Material kaufte sowie Kundenanfragen bearbeitete* [279]. Der ihm drohende Strafrahmen ist zu mildern (§§ 27 Abs. 2, 49 Abs. 1 StGB).

- Nach dieser Bewertung können sich die Täter nicht zu einer Bande zusammen geschlossen haben. Sie verlangt nach mindestens drei Mittätern. Damit scheiden die Vorwürfe des gewerbsmäßigen Bandenbetruges (§ 263 Abs. 5 StGB) und der Verabredung zu einem Verbrechen (§ 30 Abs. 2 StGB) aus. Der gewerbsmäßige Bandenbetrug droht als Verbrechen mit bis zu zehn Jahren Freiheitsstrafe im Einzelfall, die Verabredung zu ihm mit Freiheitsstrafen von drei Monaten bis zu sieben Jahre und sechs Monate (§ 49 Abs. 1 StGB).

- Alle drei Täter handelten gewerbsmäßig (Kasten oben), so dass sich jeder von ihnen die Betruge als besonders schwere Fälle zurechnen lassen muss (§§ 263 Abs. 3 Nr. 1, 28 Abs. 2 StGB).

- Ohne das gewerbsmäßige Handeln hätte das auch verwirklichte Dauerdelikt der Verwertung fremder Geschäftsgeheimnisse (§ 17 Abs. 3 UWG) eine materielle Klammerwirkung entfaltet, die alle zehn Tathandlungen zu einer materiellen Tat mit einer Höchstfreiheitsstrafe von fünf Jahren zusammengezogen hätte.

---

[279] **LG Göttingen**, Urteil vom 17.08.2009 - 8 Kls 1/09. Das könnte auch zur Mittäterschaft reichen: **BGH**, Beschluss vom 29.04.2008 - 4 StR 125/08; siehe auch **CF**, Mittäterschaft und strafrechtliche Haftung, 25.12.2009.

2.6.4.3 Selbstverständnis der Täter

Eine kurze Textpassage bei Warnecke und Knabe lässt aufhorchen [280]:

Die Täterpersönlichkeiten lassen sich vielleicht besonders gut dadurch charakterisieren, dass zwei der Haupttäter sich gut gekleidet und triumphierend grinsend in Handschellen vor dem Zugang der örtlichen JVA Göttingen-Rosdorf fotografieren ließen. Dieses Bild stellten sie ins Internet ein. Auch im Rahmen operativer Maßnahmen bestätigte sich, dass unsere Täter der festen Meinung waren, sie wären zu intelligent für die Strafverfolgungsbehörden.

Diese Erfahrung ist kein Einzelfall. Die versierten Täter, die sich der Mittel und Besonderheiten des Internets bedienen, sind häufig jung, aber erwachsen im strafrechtlichen Sinne (§ 1 Abs. 2 JGG), haben ihre jugendliche Prägung parallel zur explosionsartigen Entwicklung des Internets durchlaufen, sind mit Rollenspielen und der damit einhergehenden Erfahrung aufgewachsen, dass man zwar ein Spiel und dort auch „Leben“ verlieren, nicht aber echte Schmerzen und Tod erleiden kann. Sie haben häufig die Erfahrung gemacht, dass die virtuelle Kommunikation zwar auch mit sozialer Kontrolle, Streit und Konfrontation verbunden ist, aber keine nachhaltigen Konsequenzen erwarten lässt, zumal man seine Identität wechseln und sozusagen seine verbrannte Haut zurücklassen kann. So ist es in der Tat keine Seltenheit, dass viele der Täter im Bereich Betrug, Carding und anderen modernen Kriminalitätsformen den Eindruck haben, dass sie allen anderen und besonders der Strafverfolgung hoffnungslos und vor allem intellektuell überlegen sind. Das kann bis zu einer dissozialen Persönlichkeitsstörung mit Krankheitswert führen.

Warnecke und Knabe fordern deshalb mit einem gewissen Recht, die Strafverfolgung seitens der Polizei und der Staatsanwaltschaft zu intensivieren und organisatorisch auszubauen, indem zum Beispiel auch Schwerpunktstaatsanwaltschaften eingerichtet werden.

Das alleine wird nicht genügen, weil die Strafverfolgung in diesem Bereich nicht nur rechtliche, sondern besonders auch technische (Grund-) sowie soziale Kompetenz voraussetzt, die nicht zum Nulltarif zu bekommen sind.

---

[280] Volker **Warnecke**, Oliver **Knabe**, Abofallen und Simlockentfernung. Ermittlungstaktische Erfahrungen und rechtliche Bewertung spezieller Formen der IuK-Kriminalität, Kriminalistik 7/2011, S. 448 (kostenpflichtige Vollversion)

2.7 kommunikative Webaktivitäten

Auch kommunikative Inhalte im Internet können die Grenzen des Erlaubten deutlich überschreiten. Das zeigen die folgenden Beispiele. Sie sind Schlaglichter und können das weite Feld der IuK-Straftaten im weiteren Sinne allenfalls erahnen lassen.

2.7.1 Anleitungen zu Straftaten [281]

Schon gegen Ende des Jahres 2006 fand eine öffentliche Diskussion über Bombenbauanleitungen im Internet statt. Die Zahl der betreffenden Veröffentlichungen in deutscher Sprache soll seit März 2005 mit knapp 36.000 Webseiten bis Dezember 2006 auf etwa 208.000 angestiegen sein [282]. Wackere Stimmen forderten die Schaffung von Strafvorschriften, die längst vorhanden waren.

Bombenbauanleitungen haben ein besonderes Verbot in § 40 Abs. 1 WaffG [283]. Danach werden die Anleitungen und Aufforderungen, verbotene Waffen herzustellen, dem Umgang im übrigen gleichgestellt. Die Verbote ergeben sich aus der Anlage 2 Abschnitt 1 Nr. 1.3.4 zum WaffG und beschränken sich auf *Gegenstände, bei denen leicht entflammbare Stoffe so verteilt und entzündet werden, dass schlagartig ein Brand entstehen kann; oder in denen unter Verwendung explosionsgefährlicher oder explosionsfähiger Stoffe eine Explosion ausgelöst werden kann.* Die Strafbarkeit als solche folgt aus § 52 Abs. 1 Nr. 1. WaffG.

Darüber hinaus hat der Gesetzgeber mit § 130a StGB die Anleitung zu Straftaten und damit die Verbreitung von Schriften unter Strafe gestellt, wenn sie besonders schwerwiegender Verbrechen ermöglichen. Dazu verweist § 130a StGB auf den Straftatenkatalog in § 126 StGB, der auch neben anderen gemeingefährlichen Straftaten auch das Herbeiführen einer Sprengstoffexplosion gemäß § 308 StGB mit Ausnahme minder schweren und fahrlässiger Fälle umfasst (§ 308 Abs. 1 bis Abs. 3 StGB)

Die Kommentarliteratur zu § 130a StGB verweist im Wesentlichen auf die rechtswissenschaftliche Lehre. Mit den „Straftaten gegen die öffentliche Ordnung“ im Internet setzt sich außerdem ein Urteil des BGH auseinander [284], das einen Fall der Volksverhetzung betrifft (§ 130 StGB) und grundlegend auch für andere Straftaten aus diesem Abschnitt ist.

Unter Verweis auf die Definition von Schriften in § 11 Abs. 3 StGB, die auch Datenspeicher in elektronischer Form umfassen, widmet sich § 130a StGB allen Schriften, die ***geeignet*** sind, zu einer in § 126 Abs. 1 StGB genannten rechtswidrigen Tat anzuleiten, und umfasst gleichermaßen jene, die dazu ausdrücklich ***bestimmt*** sind (§ 130a Abs. 1 StGB), als auch die „***neutralen Schriften***“ (§ 130a Abs. 2 Nr. 1 StGB), die ohne ohne Aufforderungscharakter dazu „geeignet“ sind, als Anleitung zu diesen Taten zu dienen. Die Veröffentlichung im Internet ist unter die Verbreitungsmerkmale „verbreiten“ als aktives Zusenden (z.B. als E-Mail oder Newsletter) oder „zugänglich machen“ als Bereithalten zum Abruf (z.B. auf einer Homepage) zu fassen [285].

Die Veröffentlichung muss zunächst als Anleitung zu einer Katalogtat geeignet sein. Das setzt eine unterrichtende Vermittlung von Kenntnissen voraus, die die Katalogtat ermöglichen, ohne dass der Verfasser die Tat billigt oder zu ihrer Begehung auffordern muss. Geeignet ist die Publikation, wenn sie mehr als eine allgemeine Informationsquelle (Patentschriften, Lehrbücher) konkrete Sachverhalte zum Gegenstand hat und vollständig behandelt [286]. Deshalb können auch wissenschaft-

---

[281] Der Text beruht auf dem Aufsatz: Dieter **Kochheim**, Bombenbauanleitungen im Internet. Müssen die Strafverfolgungsbehörden einschreiten? 08.05.2007.

[282] News-Report.de, Mehr als 200.000 gefährliche Anleitungen zum Bombenbau im Internet, 06.12.2006; Martin **Fiutak**, Internet macht Bombenbau zum Kinderspiel, ZDNet.de 06.12.2006

[283] **BGH**, Beschluss vom 19.04.2011 - 3 StR 230/10.

[284] **BGH**, Urteil vom 12.12.2000 – 1 StR 184/00

[285] Fischer, § 184 StGB, Rn 23 [Verbreiten in Datennetzen]

[286] Fischer nennt als Beispiel die Heeresvorschrift zum

liche Erläuterungen technischer Art „geeignet“ sein, wenn sie auch zur Begehung rechtswidriger Taten verwendet werden können, weil sie zum Beispiel die Herstellung von Waffen, von Sprengstoff oder deren Handhabung behandeln (Gebrauchsanweisungen für Zielfernrohre und Nachtsichtgeräte, in denen die erreichbare hohe Treffergenauigkeit hervorgehoben wird).

Die Sozialadäquanzklausel in § 130a Abs. 3 StGB schließt die Verwirklichung des Tatbestandes aus. Sie verweist auf § 86 Abs. 3 StGB und damit auf künstlerische, wissenschaftliche und journalistische Schriften über die Geschichte und die Zeitgeschichte, die straffrei bleiben. Die Klausel eröffnet jedoch einen offenen Widerspruch zwischen der Eignung technisch orientierter, neutraler Schriften (§ 130a Abs. 2 Nr. 1 StGB), die den Straftatbestand erfüllen, und den privilegierten Schriften, deren Strafbarkeit tatbestandlich ausgeschlossen ist. Die Abgrenzungen im Einzelfall bereiten Schwierigkeiten.

Die Kommentarliteratur hebt die „Eignung“ soll hervor [287], so dass auch neutrale, aber als Anleitung geeignete Schriften nicht das Privileg nach Abs. 3 genießen. Die Eignung ist jedoch in beiden Tatbeständen die Voraussetzung für die Strafbarkeit. Das führt zu dem wenig einleuchtenden Ergebnis, dass neutrale wissenschaftliche Schriften strafbar sind und böswillige journalistische nicht.

Das widerspricht meines Erachtens einer verfassungskonformen Auslegung der Sozialadäquanzklausel. Schriften aus dem Schutzbereich der Kunst, Wissenschaft und Lehre können deshalb nur ausnahmsweise als Anleitung geeignet sein. Im Hinblick auf die Meinungsfreiheit wird sich die Auslegung im Einzelfall an dessen Besonderheiten, an der Form und Wortwahl und im Hinblick auf § 130a Abs. 1 StGB vor allem an den Beweggründen des Verfassers und den Rechtsgütern orientieren müssen, die die Strafnorm besonders schützen will.

„Brückensprengen im Verteidigungsfall“ [§ 130a StGB, Rn. 8].

[287] Fischer, § 130a StGB, Rn. 11, 22

2.7.1.1 Gefährdungsdelikte und ihr Tatort

Neben der Unterscheidung zwischen konkreten (z.B. Gefährdung des Straßenverkehrs, § 315c StGB) und abstrakten Gefährdungsdelikten (z.B. Trunkenheit im Verkehr, § 316 StGB) hat der BGH besonders die „abstrakt-konkreten“ Gefährdungsdelikte mit der praktischen Konsequenz betrachtet, dass Volksverhetzungen und ihnen folgend die Anleitungen zu Straftaten gemäß § 9 Abs. 1 StGB einen Erfolgsort in Deutschland haben, auch wenn der Täter Ausländer ist und im Ausland (in englischer Sprache) gehandelt hat [288].

Konkrete Gefährdungsdelikte haben ihren Erfolgsort dort, wo die Gefahr eintritt. Der inländische Erfolgsort führt gemäß § 9 Abs. 1 StGB unmittelbar zur Anwendung des deutschen Strafrechts. Wegen der abstrakten Gefährdungsdelikte ist es streitig, ob sie einen Erfolgsort haben, so dass der ausschließlich im Ausland handelnde Täter nicht dem deutschen Strafrecht unterliegt (wenn keine ausdrückliche Auslandstat gemäß §§ 4 bis 7 StGB vorliegt; das ist z.B. beim Verbreiten von Kinderpornographie der Fall: § 6 Nr. 6 StGB).

Die abstrakt-konkreten Gefährdungsdelikte (auch „potentielle“ Gefährdungsdelikte) begreift der BGH als eine Untergruppe der abstrakten, von denen sie sich dadurch unterscheiden, dass sie sich zur Störung des öffentlichen Friedens eignen, ohne dass eine bestimmte Gefahr durch sie eingetreten ist. Sie sind den konkreten Gefährdungsdelikten vergleichbar und haben einen inländischen Erfolgsort, wenn sie als Veröffentlichung im Internet jedem Nutzer in Deutschland *ohne weiteres zugänglich* sind und *gerade deutsche Internet-Nutzer ... zum Adressatenkreis der Publikationen ... gehören sollen* <S. 19>.

Die dargestellte Rechtsprechung des BGH orientiert sich an dem Tatbestand der Volksverhetzung (§ 130 StGB). Er verlangt, dass neben dem Inhalt der Schrift auch ihre Eignung darauf geprüft werden muss, ob sie den öffentlichen Frieden gefährdet. Denselben tatbestandlichen Aufbau hat der Gesetzgeber bei der Anleitung zu Straftaten ge-

[288] **BGH**, Urteil vom 12.12.2000 – 1 StR 184/00

wählt, so dass auch dieser Tatbestand als abstrakt -konkretes Gefährdungsdelikt anzusehen ist.

Für die Strafverfolgungspraxis hat das zur Folge, dass alle Anleitungen zu gemeingefährlichen Straftaten im Sinne von § 126 StGB, die in Deutschland prinzipiell erreichbar sind – und das sind alle, die öffentlich im Internet präsentiert werden – einen inländischen Erfolgsort haben und deshalb nach deutschem Strafrecht von den deutschen Strafverfolgungsbehörden verfolgt werden müssen.

2.7.1.2. Schriften in nicht deutscher Sprache

In dem vom BGH entschiedenen Fall der Volksverhetzung handelte der Täter in Australien und verfasste die Schriften in englischer Sprache. Dessen ungeachtet geht der BGH davon aus, dass sich seine Schriften an das deutsche Internetpublikum richten, weil sie *einen nahezu ausschließlichen Bezug zu Deutschland* haben.

Die Verwendung der deutschen Sprache ist somit ein starkes Indiz für den auf Deutschland gerichteten Bezug, aber kein Ausschlusskriterium. Auch für deutsche Internetnutzer wird wie für alle westlichen Teilnehmer gelten, dass Englisch die wohl am meisten verbreitete Umgangssprache im Internet ist.

Dasselbe dürfte für andere Fremdsprachen gelten, wenn mit ihnen besonders sprachliche Minderheiten oder Mehrsprachler angesprochen werden sollen. Unübliche Fremdsprachen dürften hingegen nicht zur Störung des öffentlichen Friedens geeignet sein, insbesondere dann nicht, wenn sie im fernen Osten beheimatet sind und über besondere Schriftzeichen verfügen.

Das ergibt sich auch daraus, dass Naziparolen in fremder Sprache nicht unbedingt strafbar sind (§§ 86, 86a StGB) [289]. Durch ihre Übersetzung in eine andere Sprache erfährt eine Nazi-Parole eine grundlegende Verfremdung, die der Tatbestand des § 86a StGB nicht erfasst, wenn sie nicht nur durch ihren Sinngehalt, sondern vor allem durch die deutsche Sprache ihre charakteristische Prägung erfahren hat [290].

---

[289] **BGH**, Urteil vom 13.08.2009 - 3 StR 228/09

[290] Deshalb habe ich die entsprechende Meldung so überschrieben: **CF**, 'Iw je* batlh, 16.08.2009, also mit dem Slogan, den der BGH betrachtet hat.
Zur Auflösung: Klingonisch nach GerDIC.

2.7.1.3 Geschlossene Benutzerkreise

Die Volksverhetzung und die Anleitung zu Straftaten (§§ 130, 130a StGB) heben das Verbreiten friedensstörender Inhalte hervor. Damit unterscheiden sie sich ganz besonders von dem Verbreiten gewalt-, tier- und kinderpornographischer Schriften (§§ 184a, 184b StGB), deren Herstellung und wegen der kinderpornographischen Schriften auch deren Besitz strafbar ist. Ihre Verfolgung wurde außerdem dem Weltrechtsprinzip unterstellt (§ 6 Nr. 6 StGB).

Nach der breiten Anlage der tatbestandlichen Handlungen im Zusammenhang mit pornographischen Schriften muss sich deren Strafverfolgung nicht auf den öffentlichen Teil des Internets beschränken, sondern kann auch geschlossene Nutzergruppen mit besonderen Zugangssicherungen umfassen.

Nach ihrer Ausrichtung auf die Gefährdung des öffentlichen Friedens erfordern die Volksverhetzung und die Anleitung zu Straftaten hingegen ein Handeln in einer gewissen Öffentlichkeit. Das unterscheidet sie vom „Aufstacheln zum Angriffskrieg“ (§ 80a StGB), das neben der Öffentlichkeit auch Versammlungen und Schriften als Foren nennt. Dazu gehören auch geschlossene Versammlungen, nicht aber zufällige Personenmehrheiten [291].

Ein klärendes Wort über die Qualität von Öffentlichkeit in Bezug auf geschlossene Benutzerkreise fehlt noch. Soweit auch die Schriften und Dateien im Sinne von § 11 Abs. 3 StGB angesprochen sind, richten sie sich bereits vom Wortsinn her nicht an eine offene und jedermann zugängliche „Öffentlichkeit“, sondern möglicherweise auch an eine geschlossene, aus der andere Öffentlichkeiten ausgeschlossen sind. Das dürfte dann auch die (konkrete) öffentliche Aufforderung zu (künftigen) Straftaten gemäß § 111 StGB und die Belohnung und Billigung von (geschehenen) Straftaten nach § 140 StGB betreffen (ggf. auch § 86 StGB) [292].

2.7.1.4 Fazit

Die Rechtsprechung des BGH führt zu einer starken Ausweitung der deutschen Strafgewalt, indem er einen inländischen Erfolgsort bei den abstrakt-konkreten Gefährdungsdelikten im Zusammenhang mit elektronischen Publikationen im Internet annimmt. Seine Ableitung und Auslegung sind stimmig und fachlich nicht zu beanstanden.

Das immanente Problem der Straftaten gegen den öffentlichen Frieden ist ihre Nähe zum Gesinnungsstrafrecht, indem sie als Gefährdungsdelikte formuliert sind und dem Schutz des Grundrechts der Meinungsfreiheit entgegen wirken. Das rechtfertigt nur die besondere Gefährlichkeit für das gesellschaftliche Zusammenleben und die demokratische Ordnung, die von gemeingefährlichen und schweren Straftaten oder von der Förderung des Hasses und der Herabwürdigung von Bevölkerungsteilen ausgehen.

Einer tieferen Auseinandersetzung mit der Sozialadäquanzklausel geht der BGH aus dem Weg, obwohl sie sowohl in § 130 Abs. 6 als auch in §130a Abs. 3 StGB die Strafbarkeit ausschließt. Insoweit führt er nur aus, dass die fraglichen Schriften nicht der Wissenschaft, Forschung oder Lehre dienen und nicht durch das Grundrecht auf freie Meinungsäußerung geschützt seien.

Das Spannungsfeld zwischen strafrechtlicher Eingriffstiefe einerseits und die Meinungsfreiheit, journalistische Berichterstattung und wissenschaftliche Auseinandersetzung andererseits wird die Rechtsprechung sicherlich noch weiter beschäftigen.

---

[291] Fischer, § 80a StGB, Rn 4.

[292] Die öffentliche Aufforderung und Billigung von Straftaten hat auch Bedeutung für die Teilnehmer in Carding- und anderen Boards. Beide Strafvorschriften sind meines Wissens noch nicht im Zusammenhang mit der Cybercrime betrachtet worden.

2.7.2 Gewaltfantasien im Zauberwald

Mit den bestialischen Gewaltfantasien *pädophil orientierter Menschen* in einem Internetchat (Zauberwald) hat sich der BGH auseinandersetzen müssen [293] und dabei festgestellt, dass auch solche Täter eine Verbrechensabrede treffen können (§ 30 Abs. 2 StGB), die sich nicht persönlich und nicht namentlich, sondern nur unter ihren Tarnnamen kennen. Wegen eines nur einmaligen Kontakts zwischen den Beteiligten und keiner erkennbaren Ausführungshandlungen zweifelt der BGH jedoch an einer von *ernstlichen Willen getragenen Einigung ... an der Verwirklichung eines bestimmten Verbrechens mittäterschaftlich mitzuwirken* <Rn 16> und bemängelt, das erkennende Gericht hätte die *Verbrechensfantasie von wirklichem verbrecherischen Willen und dessen Umsetzung* genauer abgrenzen müssen <Rn 18>. An dem Ergebnis gibt es in diesem Fall keine Zweifel anzumelden.

Viele der Sachverhalte, die der Rechtsprechung des BGH zugrunde liegen, betreffen den sexuellen Missbrauch, Gewalt, Raub und Mord. Sie hinterlassen – besonders hier – ein sauer aufstoßende Gefühl, das von den kranken, hemmungslosen und pädofantastischen Vorstellungen über die Entführung eines optimal achtjährigen Jungen, seines sexuellen Missbrauchs und schließlich seiner rituellen Tötung herrührt. Es fällt schwer, dabei immer einen professionellen und neutralen Standpunkt zu behalten.

Ungeachtet der strafrechtlichen Fragen gehören die beteiligten Leute nachhaltig therapiert, auch wenn sie nur aus Spaß am Fabulieren gehandelt hätten. Oh Vater, es gruselt mir [294].

2.7.3 Geschlossene Boards als öffentliche Räume [295]

In die Geflogenheiten von kinderpornographischen Foren führt uns der BGH mit einem Urteil aus dem Januar 2012 ein [296], das gleichzeitig zwei materielle Rechtsfragen klärt: Auch geschlossene Boards sind im Sinne des materiellen Kipo-Strafrechts "öffentlich" dann, wenn sich in ihnen eine beliebige Zahl von anonymen Interessierten tummeln können [297]. Ihre Betreiber machen sich auch wegen der Dateien strafbar, die sie nicht selber in Besitz nehmen, sondern zu denen sie den Mitgliedern nur den Zugang verschaffen (Drittbesitzverschaffung).

Die beiden Angeklagten waren die Administratoren von zwei nacheinander eingerichteten Boards, auf denen *Mitglieder Nachrichten oder Anfragen (sog. Postings) hinterließen und insbesondere dauerhaft und ungestört kinderpornographische Bild- und Videodateien austauschten* <Rn 3>. Die Adressen der abgelegten Dateien wurden leicht abgeändert (zum Beispiel hxxp:// anstelle von http://).

Das Board war in verschiedene Bereiche unterteilt. Ein Teil hiervon war jedermann zugänglich, im Übrigen war das Board nur Mitgliedern vorbehalten, die - graduell abgestuft - durch verschiedene Aktivitäten, insbesondere das eigene Posten von kinderpornographischen Dateien innerhalb des Boards, eine entsprechende Zugangsberechtigung erhalten hatten. Der Angeklagte N. war hierbei als "Moderator" tätig, um für "Ruhe und Ordnung" unter den Besuchern des Boards zu sorgen. Zudem brachte er in dieser Funktion zahlreiche eigene Ideen ein, um den Erhalt des "Z. "-Boards zu sichern und zu fördern <Rn 4>.

Jedenfalls in den exklusiven inneren Hard Core-

---

293 **BGH**, Beschluss vom 16.03.2011 - 5 StR 581/10

294 Frei nach Johann Wolfgang von **Goethe**, Erlkönig, 1782.

295 Dieses Kapitel wurde im März 2012 eingefügt. Siehe auch: CF, geschlossene Boards sind öffentliche Räume, 17.03.2012.

296 **BGH**, Urteil vom 18.01.2012 - 2 StR 151/11

297 Siehe auch: CF, Verbreitung von Kinderpornographie im Chat-Kanal, 04.03.2012; **BGH**, Urteil vom 08.02.2012 - 2 StR 346/11.

Bereich des späteren Boards wurden die Mitglieder nur zugelassen, wenn sie entsprechendes Material lieferten (Keuschheitsprobe). *Sofern die Mitglieder innerhalb eines bestimmten Zeitraums keine Aktivitäten entfalteten, wurde ihr Zugang automatisch deaktiviert, um passive Teilnehmer von dem Board fernzuhalten. So unterlag die Szene einem ständigen Wechsel. Am 29. September 2009 hatte das "S. "-Board aktuell 476 Mitglieder zu verzeichnen* <Rn 5>.

Die geschilderten Geflogenheiten weichen nicht sonderlich ab von denen, die sich anderer Interessen widmen (zum Beispiel dem Carding), außer im Ekelfaktor: Von den Mitgliedern wurden verstärkt *auch sog. "Eigenproduktionen", also selbst gefertigtes Bild- und Filmmaterial, gepostet, die den sexuellen Missbrauch nahestehender Personen zeigten* <Rn 5>.

2.7.3.1 Öffentlichkeit im Sinne von § 184b StGB

Das Urteil betritt mit klaren Aussagen rechtliches Neuland: *Zutreffend hat das Landgericht das Betreiben des "Z. "-Boards durch den Angeklagten N. und des "S. "-Boards durch beide Angeklagte - jeweils nebst den dazugehörigen Chats - als bandenmäßige Verbreitung kinderpornographischer Schriften in der Variante des öffentlichen Zugänglichmachens (§ 184b Abs. 1 Nr. 2 Var. 4, Abs. 3 Alt. 2 StGB) gewertet. Ein solches Zugänglichmachen liegt in der Zurverfügungstellung einer Plattform, die dem Einstellen von Dateien im Internet dient, wobei die Möglichkeit des Lesezugriffs genügt (...). Nichts anderes gilt für das Bereitstellen entsprechender Links, wobei es nach Auffassung des Senats ohne Belang ist, ob das Zugänglichmachen durch das Posten eines Links auf eine kinderpornografische Datei erfolgt (...) oder ob ... die Zieladresse durch Verändern von Buchstaben aus Sicherheitsgründen geringfügig verändert und von den Nutzern nach Weisung manuell eingegeben wird.* <Rn 9>.

Der BGH stellt klar, dass der Begriff "öffentlich" auch für die geschlossenen Teile eines Boards gilt. Das gilt bereits dann, wenn *einem größeren, in seiner Zahl und Zusammensetzung unbestimmten Personenkreis die Möglichkeit der Kenntnisnahme eröffnet wurde* <Rn 11> und vor allem wenn *ein professionell organisierter Kinderpornoring im Internet eine Tauschbörse mit mehreren tausenden Zugriffen pro Tag und vielen hundert anonymen pädophilen Mitgliedern unterhält, wobei das einzige Zugangshindernis das eigene Posten kinderpornografischer Dateien ist. Ein öffentliches Zugänglichmachen von kinderpornografischem Material liegt deshalb vor, wenn der Zugang nicht auf einen dem Anbieter überschaubaren kleinen Personenkreis beschränkt werden kann, es sich vielmehr um einen anonymen, nicht überschaubaren Benutzerkreis handelt.*

2.7.3.2 Drittbesitzverschaffung

Der BGH geht noch weiter, indem er die Board-Betreiber auch für die Drittbesitzverschaffung in Anspruch nimmt (§ 184b Abs. 2, Abs. 3 Alt. 2 StGB):

Drittbesitzverschaffen setzt zwar grundsätzlich - in Abgrenzung zum eigenen Sichverschaffen des Nutzers - voraus, dass die Handlung des Täters direkt und unmittelbar auf die Besitzverschaffung des Dritten gerichtet ist. Bedarf es aber - wie hier - nur noch einer geringfügigen Mitwirkungshandlung des Empfängers selbst, der lediglich den Link anklicken muss, um die tatsächliche Herrschaft über die kinderpornografischen Dateien zu erlangen, und ist aufgrund der gerade auf den Austausch und die Übermittlung solcher Daten gerichtete Kommunikation in einem Chat mit einer alsbaldigen Inanspruchnahme des Downloadangebots zu rechnen, ist es ohne Bedeutung, dass der letzte Schritt zur eigentlichen Besitzerlangung in der Hand des Nutzers liegt … <Rn 18>.

Danach bedeutet es für das Unternehmen des Drittbesitzverschaffens keinen Unterschied, ob der Täter dem Nutzer die Daten etwa per E-Mail mit entsprechendem Anhang (...) übermittelt oder ob er diesem die Möglichkeit des Zugriffs auf diese - wie vorliegend - durch Übermitteln eines anzuklickenden Links verschafft hat. Auch für die

Tathandlung des Verbreitens i.S.v. § 184b Abs. 1 Nr. 1 StGB macht es nach der Rechtsprechung des Bundesgerichtshofs (BGHSt 47, 55, 59 f.) keinen rechtlich relevanten Unterschied, ob der Anbieter dem Nutzer die Dateien explizit zusendet (Upload) oder der Nutzer diese durch Aktivieren eines Links anfordert (Download) <Rn 19>.

2.7.3.3 Fazit

Das Urteil hat auch eine Signalfunktion für die polizeilichen Ermittlungen in den Boards. Wenn selbst ihre zugangsbeschränkten Teile als Öffentlichkeit anzusehen sind, stellen sich die Fragen nach der Eingriffsgrundlage für Ermittlungen ohne die Schärfe, die sie hätten, wenn ein starker Schutz durch Grundrechte bestände. So greift zunächst wegen der Beobachtung des Boards die Ermittlungsgeneralklausel (§§ 161 Abs. 1 S. 1, 163 Abs. 1 S. 2 StPO). Je stärker sich die Ermittlungen auf einen bestimmten Personenkreis oder einen bestimmten Beschuldigten konzentrieren, bedarf es zunächst der Zustimmung der Staatsanwaltschaft (§ 110b Abs. 1 S. 1 StPO) oder sogar des Gerichts (§ 110b Abs. 2 Nr. 1 StPO) [298]. Die genauen Grenzen zwischen der freien Informationsbeschaffung im Internet, dem im Einzelfall beauftragten NoeP und dem Verdeckten Ermittler sind noch nicht bestimmt. Dazu bedarf es erst noch breiterer Erfahrungen.

Das größte Problem bei den Ermittlungen im KiPo-Bereich sind die Keuschheitsproben. Die Ermittler sind zwar berechtigt unerkannt zu ermitteln, nicht aber dazu, Straftaten zu begehen. Bereits der schlichte Besitz von KiPo-Abbildungen ist strafbar. Es wird die Meinung vertreten, dass die polizeiliche Verwendung kinderpornographischer Bilder durch Notstand gerechtfertigt ist (§ 34 StGB). In dieser Allgemeinheit teile ich die Auffassung nicht. Wenn jedoch bekannt ist, dass - wie im vom BGH entschiedenen Fall - neue "Eigenproduktionen" gepostet werden, wird auch davon ausgegangen werden können, dass sexueller Missbrauch an Kindern akut stattfindet. Das könnte in der Tat eine gegenwärtige, nicht anders abwendbaren Gefahr für Leben oder Leib sein, die einen Notstand begründet.

---

[298] Siehe wegen der Einzelheiten: Dieter **Kochheim**, Verdeckte Ermittlungen im Internet, # 1.20, März 2012.

2.7.4 Speichern im Cache

Das öffentliche Verbreiten, Anbieten und Zeigen pornographischer Schriften und Dateien (§ 11 Abs. 3 StGB) ist gemäß § 184 StGB strafbar, wenn sie dadurch Jugendlichen und Kindern zugänglich gemacht werden. Das Pornographieverbot hat vor allem auch Eingang in den Jugendmedienschutz-Staatsvertrag – JMStV – gefunden (§ 4 Abs. 2 S. 2 JMStV) und wirft immer wieder Fragen auf, zum Beispiel nach einem effektiven Zugangsschutz [299] oder nach Websperren gegen kinderpornographische Darstellungen [300]. Daneben ist die Verbreitung gewalt- und tierpornographischer (§ 184a StGB) und sogar der Erwerb und ***Besitz*** kinderpornographischer (§ 184b StGB) sowie, zuletzt eingeführt, auch jugendpornographischer Schriften (§ 184c StGB) mit Strafe bedroht, wobei die Strafbarkeit von Erwerb und Besitz kinder- und jugendpornographischer (auch gespielter oder sonstwie wirklichkeitsnaher) Darstellungen zum Schutz der sexuellen Selbstbestimmung von Kindern und Jugendlichen tief in die persönliche Lebensgestaltung der Täter greift (§§ 184b Abs. 4, 184c Abs. 4 StGB).

Der Erwerb und der Besitz kinderpornographischer Bilder drückt sich bereits darin aus, dass sich der Täter ihre lokale Verfügbarkeit sichert, so der BGH [301]: *Auch mit der bloßen Speicherung solcher Dateien im Cache-Speicher eines PC-Systems erlangt dessen Benutzer Besitz (...), weil es ihm möglich ist, jederzeit diese Dateien wieder aufzurufen, solange sie nicht manuell oder systembedingt automatisch gelöscht wurden.*

Dem häufig geäußerten Einwand, gegen untergeschobene Dateien und die Zwischenspeicherung von Webseiten, die ohne Ahnung von ihrem wirklichen Inhalt aufgerufen wurden, könne sich der Anwender nicht wehren, ist mit dem Bürgerlichen Gesetzbuch zu begegnen: Nach § 854 Abs. 1 BGB erlangt Besitz an einer Sache, wer die tatsächliche Gewalt über sie erwirbt. Das setzt einen natürlichen Besitzerwerbswillen voraus, der sich in der schlichten Handlung des an sich Nehmens ausdrückt [302].

Gegen einzelne Abbildungen im Zwischenspeicher wird deshalb der Einwand des „Zufalls“ greifen, nicht aber gegen eine Vielzahl von ihnen. Sie lassen erkennen, dass der Betroffene den Zwischenspeicher systematisch zur Ablage und zum Wiederaufruf nutzt [303].

---

[299] Deutliche Worte und hohe Anforderungen kommen vom **BGH**, Urteil vom 18.10.2007 - I ZR 102/05.

[300] **CF**, Sperrung von Webseiten, 19.04.2009;
CF, [rechtswidrige] Verweigerung, 29.11.2009.

[301] **BGH**, Beschluss vom 10.10.2006 - 1 StR 430/06

[302] Wegen der emsigen Helfer, die nur der Strafverfolgung helfen wollen: **CF**, gutgläubige Helfer, 25.12.2007.

[303] Die Ausreden erinnern an die emsigen Diskussionen um „Disclaimer“, also den (fadenscheinigen) Haftungsausschlusserklärungen, die die wohl berühmteste Gerichtsentscheidung im Internet ausgelöst hat: **LG Hamburg**, Urteil vom 12.05.1998 - 312 O 85/98.
Das LG Hamburg hat nur gesagt, dass derjenige, der ganz gezielt beleidigende Quellen im Internet zu bestimmten Personen zusammenstellt, sich irgendwann nicht mehr herausreden kann, weil er sich die fremden, misswertenden Urteile zu Eigen macht.

2.7.5 Nazipropaganda im Internetradio

Die Angeklagten haben systematisch auf Streaming-Plattformen (Internet-Radio) rechtsradikale Musik und andere Propaganda gesendet. Sie wurden deshalb auch wegen der Bildung einer kriminellen Vereinigung (§ 129 StGB) verurteilt [304]. Der BGH verfeinert aus diesem Anlass seine Rechtsprechung zu dem Organisationsdelikt und passt sie der zur Bande an:

Schließen sich mehrere Täter zu einer kriminellen Vereinigung zusammen, hat dies - entsprechend den bei einem Zusammenschluss als Bande geltenden Grundsätzen - nicht zur Folge, dass jede von einem Vereinigungsmitglied begangene Tat den anderen Mitgliedern ohne weiteres als gemeinschaftlich begangene Straftat im Sinne des § 25 Abs. 2 StGB zugerechnet werden kann. Vielmehr ist für jede einzelne Tat nach den allgemeinen Kriterien festzustellen, ob sich die anderen Mitglieder hieran als Mittäter, Anstifter oder Gehilfen beteiligt oder ob sie gegebenenfalls überhaupt keinen strafbaren Tatbeitrag geleistet haben (vgl. BGH, Beschlüsse vom 24. Juli 2008 - 3 StR 243/08 ...; vom 13. Mai 2003 - 3 StR 128/03 …) <Rn 15>

Haben bei einer durch mehrere Personen begangenen Deliktsserie einzelne Angeklagte einen Tatbeitrag zum Aufbau oder zur Aufrechterhaltung einer auf die Begehung von Straftaten ausgerichteten Infrastruktur erbracht, sind die Einzeltaten der Mittäter zu einem uneigentlichen Organisationsdelikt zusammenzufassen, durch welches mehrere Einzelhandlungen rechtlich verbunden und hiermit die auf Grundlage dieser Infrastruktur begangenen Straftaten in der Person der im Hintergrund Tätigen zu einer einheitlichen Tat oder gegebenenfalls zu wenigen einheitlichen Taten im Sinne des § 52 Abs. 1 StGB zusammengeführt werden (BGH, Urteil vom 17. Juni 2004 - 3 StR 344/03 ...; Beschluss vom 21. Dezember 1995 - 5 StR 392/95, ...; Beschluss vom 26. August 2003 - 5 StR 145/03 ...). <Rn 16>

Die im Rahmen einer kriminellen Vereinigung begangenen Taten stehen zueinander im Verhältnis der Tateinheit, da die mitgliedschaftliche Beteiligung in einer solchen Vereinigung zu deren Verklammerung führt. Voraussetzung für eine solche Klammerwirkung ist, dass die Ausführungshandlungen zweier oder mehrerer an sich selbstständiger Delikte zwar nicht miteinander, wohl aber mit der Ausführungshandlung eines dritten Tatbestandes (teil)identisch sind und dass zwischen wenigstens einem der beiden an sich selbstständigen Delikte und dem sie verbindenden, sich über einen gewissen Zeitraum hinziehenden (Dauer-) Delikt zumindest annähernde Wertgleichheit besteht ([305]...). Als Maßstab hierfür dient die Abstufung der einzelnen Delikte nach ihrem Unrechtsgehalt unter Orientierung an den Strafrahmen, wobei der Wertevergleich nicht nach einer abstrakt-generalisierenden Betrachtungsweise, sondern anhand der konkreten Gewichtung der Taten vorzunehmen ist (...). <Rn 17>

Das bedarf der Erläuterung.

---

[304] **BGH**, Beschluss vom 19.04.2011 - 3 StR 230/10, [zitiert als „BGH 2011“] Rn 14

[305] Verweis auf: **BGH**, Beschluss vom 02.12.2008 - 3 StR 203/08.

2.7.5.1 kriminelle Vereinigung

Eine Vereinigung ist ein auf Dauer angelegter freiwilliger Zusammenschluss von mindestens drei Personen, die unter dem Willen der Gesamtheit gemeinsame Zwecke verfolgen und sich als einheitlicher Verband fühlen [306]. Sie bedarf einer festen Organisation, die Unterordnung der Beteiligten unter einen Gruppenwillen und verbindliche Regeln für die Willensbildung [307]. Daran fehlt es, wenn es allein darum geht, den Willen eines Anführers durchzusetzen [308]. § 129 Abs. 1 StGB ist ein Vergehen und benennt mehrere Begehungsformen:

- Die Gründung einer kriminellen Vereinigung, wobei nicht jede zustimmende Willensbekundung die Beteiligung an der Gründung rechtfertigt, sondern nur die wesentliche Förderung [309].
- Beteiligung an einer kriminellen Vereinigung, die sich in aktiven Handlungen zur Förderung von Aufbau, Fortdauer oder Tätigkeit ausdrücken muss [310]. Gründung und Beteiligung stehen nicht notwendig in Tateinheit, besonders dann nicht, wenn der Zeitpunkt für die Gründung und ihre Umstände im einzelnen unbekannt sind [311]. Die Beteiligung kann sich auf die Ausführungstaten oder auf die Förderung der Organisation als solche richten (Rekrutierung, Ausbildung, Betrieb von Infrastruktur).
- Unterstützung einer kriminellen Vereinigung. Es handelt sich um eine zur Täterschaft verselbständigte Beihilfe zur Mitgliedschaft. Sie betrifft Nichtmitglieder und muss über eine „Sympathiewerbung“ hinaus gehen und auf die Förderung der Organisation als solche gerichtet sein [312].
- Werbung um Mitglieder oder Unterstützer. Werber kann nur ein Nichtmitglied sein, das Personen für die Organisation zu gewinnen versucht.

§ 129 Abs. 4 S. 1 erster Halbsatz StGB benennt zwei qualifizierte (selbständige) Tatbestände [313], indem die „Rädelsführer“ und die „Hintermänner“ einer im Mindestmaß erhöhten Freiheitsstrafe von sechs Monaten unterworfen werden. Die sonstigen besonders schweren Fälle <zweiter Halbsatz> sind unbenannt. Die Förderung der kriminellen Organisation hat zwei Schwerpunkte, die Ausführung der Taten, zu deren Zweck sie sich gebildet hat, und die Förderung der Organisation als solche, an der besonders die „Hintermänner“ beteiligt sind.

Der BGH wendet auf die Tathandlungen im Rahmen der kriminellen Vereinigung die Grundsätze an, die auch für die Bande gelten, so dass den Tätern nur ihre eigenhändigen Anteile als Mittäter, Anstifter und Gehilfen zuzurechnen sind [314]. Eine generelle Zurechnung nach Maßgabe von § 25 Abs. 1 StGB erfolgt nicht.

Tatbeiträge, die sich auf die Infrastruktur der Organisation beziehen, fassen die Handlungen zu einem uneigentlichen Organisationsdelikt zusammen, so dass diese Täter grundsätzlich wegen einer tateinheitlichen Tat zu bestrafen sind (*oder gegebenenfalls zu wenigen einheitlichen Taten … zusammengeführt* [315]). Dieses Handlungsmodell ist sehr ähnlich dem, das der BGH für die fördernde Mittäterschaft in einer Bande entwickelt hat (Beschaffung eines Firmenmantels für mehrere Betrugstaten [316]).

Die Mitgliedschaft im Sinne von § 129 StGB ist kein „Zustandsdelikt“ nach dem Vorbild des verbotenen Waffenbesitzes, wobei durch eine einmalige Handlung ein rechtswidriger Zustand herbeigeführt wird, sondern ein Handlungsdelikt, das Aktivitäten des Täters voraussetzt. Deshalb ist besonders wegen der Ausführungstaten im Einzelfall zu fragen, durch welche Handlungen der Täter die

---

306 Fischer, § 129 StGB, Rn 6

307 Fischer, § 129 StGB, Rn 7

308 Leitbild: Charismatischer Räuberhauptmann.

309 **BGH**, Beschluss vom 10.01.2006 - 3 StR 263/ 05, Leitsatz 4

310 Fischer, § 129 StGB, Rn 24

311 **BGH** 2011, Rn 19

312 Fischer, § 129 StGB, Rn 30

313 Fischer, § 129 StGB, Rn 41

314 **BGH** 2011, Rn 15

315 **BGH** 2011, Rn 16

316 **BGH**, Beschluss vom 29.04.2008 - 4 StR 125/08

Vereinigungsziele gefördert hat. Sind das immer wieder neue Handlungen ohne maßgebliche, andauernde Wirkung, dann spricht das dafür, dass keine Klammerwirkung eintritt.

2.7.5.2 Klammerwirkung

Die im Rahmen einer kriminellen Vereinigung begangenen Taten stehen zueinander im Verhältnis der Tateinheit, da die mitgliedschaftliche Beteiligung in einer solchen Vereinigung zu deren Verklammerung führt [317].

Damit entsteht die schon im Zusammenhang mit der ▸ Göttinger Abofalle angesprochene Klammerwirkung. Sie kann nicht nur verschiedene materielle Taten tateinheitlich verbinden, sondern auch wegen erst später bekannt werdender Delikte einen Strafklageverbrauch eintreten lassen, wenn es in Tateinheit mit einer Mitgliedschaft in einer kriminellen Vereinigung steht (§ 129 StGB). Das ist der Fall, wenn zwischen den Taten zumindest eine annähernde Wertgleichheit besteht [318]. Das hat der BGH an anderer Stelle auch für die Strafvereitelung angenommen, die mehrere Verunglimpfungen, Beleidigungen und Nötigungen zu einer vom gemeinsamen Vereitelungswillen getragenen Tat zusammen fasst [319], im Verhältnis zwischen Betrug (§ 263 StGB) und strafbarer Werbung (§ 16 UWG) eine Klammerwirkung durch die Wettbewerbstat aber abgelehnt [320].

Aber: *Eine minder schwere Dauerstraftat hat nicht die Kraft, mehrere schwerere Einzeltaten, mit denen sie ihrerseits jeweils tateinheitlich zusammentrifft, zu einer Tat im Sinne des § 52 Abs. 1 StGB zusammenzufassen* [321]. Danach ist es grundsätzlich ausgeschlossen, dass ein Vergehen mehrere Verbrechen zu einer Tat zu verklammert [322]. Auch wenn der BGH eine *konkrete Gewichtung der Taten* verlangt und sich gegen eine *abstrakt-generalisierenden Betrachtungsweise* ausspricht [323], treten jedenfalls vom Grundsatz her keine Klammerwirkung und kein Strafklageverbrauch durch das Grunddelikt nach § 129 Abs. 1 StGB ein, wenn mehrere Verbrechen oder besonders schwere Fälle mit Höchststrafen von mehr als fünf Jahre Freiheitsstrafe als Ausführungstaten in Tateinheit mit einer Mitgliedschaft in einer kriminellen Vereinigung stehen [324]. Besonders im Hinblick auf die beiden Qualifikationstatbestände – Rädelsführer und Hintermänner, die immer ein Vergehen bleiben (auch nach § 129 Abs. 4 S. 1 [nach dem Semikolon] StGB) – und sonstigen besonders schweren Fälle kann die Klammerwirkung sehr schnell eintreten, wenn die Ausführungstaten ihrerseits Vergehen sind und geringe Höchststrafen vorsehen.

---

317 **BGH** 2011, Rn 17

318 **BGH** 2011, Rn 17

319 **BGH**, Beschluss vom 02.12.2008 - 3 StR 203/08, Rn 17

320 **BGH**, Beschluss vom 09.11.2011 - 4 StR 252/11, S. 8

321 **BGH**, Beschluss vom 10.11.2010 - 5 StR 464/10, Rn 3

322 **BGH**, Urteil vom 11.06.1980 - 3 StR 9/80, Rn 8

323 **BGH** 2011, Rn 17

324 Siehe auch: **BGH**, Beschluss vom 13.09.2011 - 3 StR 196/11, Rn 24.

2.7.5.3 kriminelle Vereinigungen zu IuK-Straftaten

Die Tatsachengerichte zeigen traditionell eine gewisse Zurückhaltung, wenn es darum geht, schwerere Strafgesetze anzuwenden, die die organisatorische Gefahr von kriminellen Verbünden hervorheben. Das gilt für die Bandendelikte [325] und mehr noch für die Verabredung zu einem Verbrechen [326] (§ 30 StGB) sowie die kriminelle Vereinigung [327] (§ 129 StGB). Anders der BGH, der immer häufiger auf die Organisationsregeln anspricht, ihre Anwendungsbereiche umreißt und präzisiert und damit deutliche Signale für die strafrechtliche Behandlung von IuK-Straftaten setzt. So betrachtet er die Abgreifer beim Skimming wegen ihrer professionellen Handlungen und wesentlichen Tatanteile grundsätzlich als Mittäter [328] und lässt den Versuch der Fälschung von Zahlungskarten mit Garantiefunktion in arbeitsteiligen Tätergruppen bereits beim Übermitteln der ausgespähten Daten beginnen [329]. Im Zusammenhang mit dem ▸ Zauberwald verlangt er zwar nach einer sauberen Abgrenzung zu reinen Gewaltfantasien, stellt jedoch eine Verbrechensabrede in Kommunikationsforen im Internet nicht in Zweifel. Schließlich zeigt das ▸ Streaming-Beispiel, dass die Schwelle zur kriminellen Vereinigung schnell überschritten ist.

Die Erscheinungsformen des IuK-Strafrechts sind häufig mit lockeren (▸ Webshops) oder festen, arbeitsteiligen Gruppen verbunden (▸ ebenda), die eine besondere Organisationsgefahr entstehen lassen, die auch schon leitend für die Neuausrichtung des Bandenstrafrechts gewesen ist [330].

Vor allem die mehr oder weniger geschlossenen Boards, die sich hemmungslos der Verwirklichung von Straftaten widmen, werden sich verstärkt an ihrer Organisationsform und an „exotischen“ Straftaten wie die öffentliche Aufforderung zu (künftigen) Straftaten gemäß § 111 StGB und die Belohnung und Billigung von (geschehenen) Straftaten nach § 140 StGB messen lassen müssen.

Der Tatbestand zur kriminellen Vereinigung nach § 129 StGB ist ein Staatsschutzdelikt nach § 74a GVG und deshalb besonderen Kammern des Landgerichts vorbehalten, dessen Bezirk auch ein Oberlandesgericht beherbergt. Dem folgt auch die staatsanwaltschaftliche Zuständigkeit.

Im Zusammenhang mit der Verfolgung mafiöser Strukturen unter den Dieben im Gesetz [331] hat der BGH unlängst Zweifel daran angemeldet, dass es sich um inländische oder europäische kriminelle Vereinigungen handelt, sondern um eine außereuropäische [332]. In diesen Fällen bedarf es einer ausdrücklichen Strafverfolgungsermächtigung (§ 77e StGB) vom Bundesjustizministerium (§ 129b Abs. 1 S. 3 StGB).

Ungeachtet dessen weitet der BGH die organisierte Beteiligung an Straftaten unter dem Begriff „uneigentliche Organisationsdelikte“ immer stärker aus [333]. Das zeigt sich auch in der jüngeren Rechtsprechung zu den kinderpornografischen Boards [334] und könnte darauf hinauslaufen, dass die Veranstalter von Webauftritten jedenfalls dann immer stärker in die strafrechtliche Haftung genommen werden, wenn sie verblümt die Möglichkeiten oder die Foren für die Straftaten anderer schaffen.

---

[325] Es gibt mindestens 51 Tatbestände, die die bandenmäßige Begehung einer höheren Strafdrohung unterwerfen: **CF**, Bandenliste, 17.01.2010.

[326] Der BGH kennt wenig Zurückhaltung und nutzt die Verbrechensabrede auch zur Lösung von Zuständigkeitsproblemen: **CF**, Der versteckte Tatort, 03.07.2011;
BGH, Beschluss vom 14.04.2011 - 1 StR 458/10.

[327] Besondere Zuständigkeit der Staatsschutzkammer nach § 74a Abs. 1 Nr. 4. GVG.

[328] **BGH**, Urteil vom 17.02.2011 - 3 StR 419/10, Rn 4

[329] **BGH**, Urteil vom 27.01.2011 - 4 StR 338/10

[330] **BGH**, Beschluss vom 22.03.2001 – GGSt 1/00

[331] CF, kriminelle Vereinigungen unter Dieben im Gesetz, 06.01.2012

[332] **BGH**, Beschluss vom 13.09.2011 - 3 StR 231/11; im wesentlichen gleich lautender Beschluss: **BGH**, Beschluss vom 13.09.2011 - 3 StR 262/11.

[333] CF, uneigentliche Organisationsdelikte, 25.02.2012

[334] Siehe: Geschlossene Boards als öffentliche Räume.

2.8 Beutesicherung

Mit dem Phishing erblickten Finanzagenten das Licht der Öffentlichkeit und erlangte auch Western Union Bekanntheit [335]. Dieses und einige wenige andere Unternehmen (z.B. MoneyGram), haben sich auf den weltweiten Bargeldtransfer spezialisiert und ermöglichen mit ihrem Filialnetz die unkomplizierte Auszahlung der Transferbeträge fast ohne Zeitverzug. Sie sind ein Segen zum Beispiel für Leute, die ihre Angehörigen in der Dritten oder an abgelegenen Stellen der Welt finanziell unterstützen wollen, eignen sich aber auch dazu, ertrogenes Geld schnell zu den Hinterleuten zu bringen. Western Union hat inzwischen starke Sicherheitsmechanismen entwickelt und kämpft noch immer gegen das schlechte Image, ein willfähriges Instrument der Geldwäsche und Beutesicherung zu sein [336].

In den ersten Berichten über die Underground Economy spielte vor allem E-Gold eine besondere Rolle [337]. E-Gold, E-Silver und E-Platinium sind Verrechnungssysteme gewesen, die ihren Kunden die Wertdeckung mit Edelmetallen versprachen und weltweite, unmittelbare Transaktionen ermöglichten [338]. Die Konten wurden auf Guthabenbasis nicht in Währungseinheiten, sondern in Edelmetallmengen geführt, so dass die örtlichen Wechselkurse schwankten, weil sie von den aktuellen Weltmarktpreisen abhingen.

Ihr Anbieter ist bis November 2009 die US-Firma e-gold Ltd. mit Sitz auf der Karibikinsel Nevis gewesen. Ihre Betreiber wurden 2008 wegen Geldwäsche verurteilt. Das Unternehmen hatte die Deckung aller Einlagen mit ihren Nennwerten durch Edelmetalle versprochen, ohne dass eine effektive Staatsaufsicht oder Prüfung durch eine anerkannte Wirtschaftsprüfungsgesellschaft bekannt geworden ist.

Virtuelle Welten wie Second Life kennen eigene Geldsysteme wie die Linden Dollars, die in dem Spiel als Tauschwert akzeptiert werden [339]. Entsprechende Verrechnungssysteme sind aus Online-, Baller- und Kampfspielen bekannt. Dort können Spielfortschritte und Ausstattungsmerkmale erworben und eben auch gekauft werden [340]. Sie haben deshalb Schnittstellen, über die Ein- und Auszahlungen abgewickelt werden können, wobei die Werthaltigkeit der Forderungen vom Vermögen des Veranstalters abhängt. Sie sind als Zwischenstationen zur Geldwäsche geeignet, auch wenn das zu einem Totalverlust führen kann, weil der Betreiber nicht unbedingt ein freundlicher Kaufmann ist, dem das Wohl seiner Kunden am Herzen liegt.

Das ist vergleichbar mit den Online-Casinos. Sie sind auf den Geldumsatz angewiesen und müssen im Interesse ihrer Attraktivität dafür Sorge tragen, dass Geld auch wieder an die Spieler zurückfließt. Ein paar verlorene Einsätze spielen für die Geldwäscher eigentlich keine Rolle – auch wenn sich einzelne Szene-Teilnehmer darüber erbosen, dass sie sich tatsächlich bei einigen Spielen das Geld aus der Tasche ziehen lassen müssen. Es gilt der alte Grundsatz, dass immer die Bank gewinnt und nicht der Spieler (alle anderen Beispiele sind Filmgeschichten).

---

335 **CF**, Auslandsüberweisungen per Bargeldtransfer, 2007

336 Die Identität eines Zahlungsempfängers im fernen Ausland bleibt weiterhin offen, weil sich unter anderem der Auszahlungsort nur grob einschränken lässt. eBay warnt deshalb seine Kunden vor ▸ verbotenen Zahlungsmethoden.

337 Moritz **Jäger**, Das Netz der Phisher: Wie Online-Betrüger arbeiten, tecchannel 20.09.2006

338 **CF**, Verrechnungssysteme auf der Basis von Edelmetallen, 2007.
Übersicht über den Zahlungsverkehr und die Zahlungssysteme: Dieter **Kochheim**, Grenzüberschreitender Transfer von Vermögenswerten, 15.05.2007.

339 **CF**, Bankenkrach in der Zweiten Welt, 20.08.2007

340 Die Tauschwerte virtueller Gegenstände wie Mobiliar in einem VR-Hotel oder einem ganzen Raumschiff führen auch zu der Frage, wie ihr Diebstahl zu behandeln ist:
CF, Diebstahl virtueller Sachen, 15.11.2007;
CF, Diebstahl in Online-Spiel, 01.02.2009;
CF, Diebstahl von Spielgeld, 07.07.2009.
Die Krone davon ist der **CF**, virtuelle Mord, 31.10.2008.

2.8.1 Agenten und Scheinadressen

Im Zusammenhang mit dem Phishing tauchte erstmals auch der Begriff „Finanzagent“ auf. Er stellt ein Bankkonto zur Verfügung, an das ertrogene Überweisungen gesandt und vom Agenten an den Täter weiter geleitet werden. Der Jargon-Begriff dafür ist wenig freundlich und heißt „Mule“, also Esel. Er wird zweimal bestraft. In den meisten Fällen wird der ertrogene Betrag seinem Konto zurückbelastet und eine Strafe wegen leichtfertiger Geldwäsche (§ 261 Abs. 5 StGB) folgt ebenfalls regelmäßig. Finanzagenten sind deshalb schnell verbrannt und müssen durch andere ersetzt werden. Sie sind eben Kanonenfutter.

Die Strafbarkeit von Finanzagenten wird gelegentlich auch aus dem Verbot unerlaubter Bankgeschäfte abgeleitet (§ 54 Abs. 1 Nr. 2 KWG). Diese Strafnorm setzt aber erlaubnispflichtige Bankgeschäfte nach § 32 Abs. 1 S. 1 KWG voraus. Solche liegen nur vor, wenn sie gewerbsmäßig oder in einem Umfang betrieben werden, *der einen in kaufmännischer Weise eingerichteten Geschäftsbetrieb erfordert*. „Gewerbsmäßig“ ist hier aber nicht strafrechtlich, sondern handelsrechtlich gemeint und erwartet einen regelrechten Handelsbetrieb. Einen solchen können Finanzagenten nicht aufbauen, weil sie bereits nach wenigen Einsätzen verbrannt sind und auffliegen.

Im Ergebnis gilt dasselbe für die Paketagenten. Sie wurden noch 2006 als Hirngespinst abgetan [341]. Zwei Handlungsmodelle haben sich für sie herausgebildet: Entweder nehmen sie Warensendungen, die durch Identitätsdiebstahl computerertrogen wurden, nur entgegen oder sie leiten sie an den Täter oder weitere Zwischenstationen weiter. Die Rechtsprechung hat keine Schwierigkeiten damit, das entweder als Geldwäsche (§ 261 StGB, [342]), als Hehlerei (§ 259 Abs. 1 StGB) oder – nicht minder strafbar – als Absatzhilfe zu betrachten [343].

Eine Variante vom Paketagenten sind Paketstationen, die sich zum anonymen Versand ertrogener oder von Handelswaren eignen, wenn sie unter falschen Identitäten eingerichtet oder die Zugangsrechte im Wege des Identitätsdiebstahls anderen gestohlen werden. Auch grenzüberschreitende Nachnahmesendungen und andere Formen des Postversands werden im Bereich der Underground Economy genutzt, wobei es immer darauf ankommt, mindestens einen der Beteiligten im Anonymen zu halten. So kommt es häufig vor, dass Briefkästen zu leerstehenden Wohnungen neue Namensaufkleber zeigen oder fabrikneue Briefkästen in Abbruchhäusern angebracht sind und zum Empfang von Kontoeröffnungsunterlagen oder anderem Schriftverkehr dienen.

Seither haben die IuK-Täter vor allem anonymisierte Formen der Beutesicherung und Geldwäsche entwickelt (§ 261 StGB). Statt echte Finanzagenten einzusetzen, lassen sie Leute mit gefälschten Personalpapieren Konten eröffnen (§ 267 StGB) und missbrauchen dazu auch Arbeitssuchende aus dem europäischen Ausland, die für ein Handgeld ihre echten Personalien zur EMA-Anmeldung und zur Eröffnung von Bankkonten zur Verfügung stellen. Falsche Personalpapiere sind billig zu haben, lassen sich – jedenfalls als digitales Abbild – einfach herstellen und Dank Photo-Shop ohne langjährige Übung verändern (▸ Urkunde und Abbild).

---

[341] **CF**, Transfer von Sachwerten, 2007

[342] Die Geldwäsche macht keinen Unterschied zwischen realem Geld, Buchgeld und anderen Gegenständen. Insoweit ergeben sich tatsächlich Überschneidungen zur Hehlerei.

[343] Einzelheiten: Dieter **Kochheim**, Der Hehler ist kein Stehler. Hehlerei und Absatzhilfe, 11.11.2009.

2.8.2 graue Bezahlsysteme

Der Handel im Internet ist auf Zahlungssysteme angewiesen, mit denen vor allem Kleinbeträge kostengünstig und sicher abgewickelt werden können. Das Micropayment der etablierten Fiinanzwirtschaft hatte – jedenfalls bis 2008 – erhebliche Anlaufschwierigkeit, um auf dem Markt Fuß zu fassen [344]. Durchgesetzt hat sich vor allem die eBay-Tochter PayPal [345], die frühzeitig auch eine Banklizenz erwarb, um Bankgeschäfte abwickeln zu können [346]. Inzwischen hat auch der Gesetzgeber reagiert und die E-Geld-Institute sowie die E-Geld-Agenten besonderen Meldepflichten im Zusammenhang mit der Geldwäsche unterworfen [347].

Die „grauen Bezahlsysteme“ sind eine bunte Mischung aus legalen Einrichtungen, die für kriminelle Zwecke missbraucht werden können, und solchen Lösungen, die sich einer Kontrolle durch Staaten und Wirtschaftsprüfungen entziehen. Die Auseinandersetzungen mit ihnen bleiben bewusst an der Oberfläche und sollen nur ihre Funktionsweise und Grenzen aus der Sicht der Nutzer beschreiben [348]. Sie fußen auf den Beschreibungen von ▸ casial.net. Seine Betreiber bezeichnen sich als eine *Gruppe aktiver Spieler*, die seit 2003 Online-Casinos testet und bewertet. Sie verzichten auf ein Impressum und die einfachen Analyse-Werkzeuge führen zu nichtssagenden Massenanbietern wie GoDaddy als Domainverwalter und ThePlanet als Hoster. Man will also eher im Anonymen bleiben.

Beschreibungen bei ▸ casial.net

▸ Click2Pay	Guthabenkonto mit banküblichen Schnittstellen
▸ ClickandBuy	Kreditkonto mit monatlicher Schlussrechnung gegen ein Bankkonto
▸ ECOcard	Guthabenkonto mit banküblichen Schnittstellen
▸ Entropay	virtuelle VISA-Kreditkarte auf Guthabenbasis
▸ GiroPay	Zahlungskarte
▸ Kreditkarte	Zahlungskarte ohne Rückzahlungsschnittstelle
▸ MoneyBookers	Guthabenkonto mit banküblichen Schnittstellen
▸ myCitadel	Guthabenkonto mit geschlossenem Teilnehmerkreis und Auszahlung per Scheck
▸ Neteller	Kreditkarte auf Guthabenbasis mit hohen Gebühren und limitiertem Umsatz
▸ PaysafeCard	Voucher (Bezugsschein) mit eindeutigem Ausgabewert und Restwertverwaltung für einen geschlossenem Teilnehmerkreis.
▸ Payspark	Kreditkarte auf Guthabenbasis, die zwei Unterkonten (Soll und Haben) zu einem Kontokorrentkonto anspricht. Das Habenkonto verliert an Wert durch hohe Gebühren und wird schließlich geschlossen.
▸ Sofortüberweisung	stellvertretende Verfügung beim Onlinebanking mit eigenen Zugangsdaten
▸ Überweisungen	normale Anweisung
▸ ukash	Voucher (Bezugsschein) mit eindeutigem Ausgabewert und Restwertverwaltung für einen geschlossenem Teilnehmerkreis.
▸ UseMyBank	Guthabenkonto mit banküblichen Schnittstellen
▸ WebMoney	Guthabenkonto mit irreversiblen, passwortgeschützten Transaktionen. Schnittstellen bestehen zu anderen virtuellen Bezahlsystemen und Wechselstuben, in denen Ein- und Auszahlungen bar abgewickelt werden.

Diesen Leuten geht es aber darum, Geld einzusetzen und Spielgewinne zu realisieren. Ihr Interesse ist dasselbe, das auch für die Underground Economy leitend ist: Geld schnell verschieben und realisieren. Deshalb ist die Rubrik ▸ Kasse besonders interessant, weil hier verschiedene kommerzielle Bezahlsysteme beschrieben und bewertet werden.

[344] **CF**, Bezahlen im Internet, 19.06.2008; **CF**, neue Bezahlverfahren, 17.12.2007.

[345] **CF**, Billing-Systeme, 2007

[346] Bankgeschäfte und Finanzdienstleistungen nach § 1 Abs. 1, Abs. 1a KWG.

[347] **CF**, Geldwäsche und E-Geld-Agenten, 09.07.2011

[348] **CF**, graue Bezahlsysteme, 08.12.2010

Überweisungen dauern zu lange. Die Zocker empfehlen statt dessen Web-Wallets von Money Bookers oder Neteller.

Das britische Unternehmen MoneyBookers bietet verschiedene Transaktionsformen an, neben dem normalen Giroverkehr auch den Geldtransfer per Computer und Kreditkarte auf Guthabenbasis sowie das eWallet. Es setzt ein Guthaben voraus und bietet eine verzögerungsfreie Verrechnung mit dem Konto eines anderen Kunden bei MoneyBookers an. Das ist so ähnlich wie früher bei E-Gold und anderen Verrechnungssystemen auf Edelmetallbasis.

Neteller ist ebenfalls ein Verrechnungssystem auf Guthabenbasis. Die Auszahlung erfolgt auch auf Kreditkarten auf Guthabenbasis und ist richtig teuer: 7,50 € pauschal für die Auszahlung und für jede Überweisung 1,9 % des Betrages.

WebMoney beschreiben die Zocker zurückhaltend und liebevoll. Zurückhaltend insoweit, weil zu den Transaktionen keine richtigen Details genannt werden. Andererseits ist das Verrechnungssystem russisch konsequent: Eine Anweisung kann nicht rückgängig gemacht, aber mit einem Kennwort geschützt werden. Das erfährt der Partner erst dann, wenn er seine Leistung erbracht hat. Bei 4,5 Millionen Nutzern weltweit läppern sich auch die Gebühren in Höhe von 0,8 % pro Verfügung. In Hackerkreisen wird der Dienst als zu teuer empfunden.

Normale Kreditkarten sind die einfachste Methode zur Zahlung. Gewinne lassen sich mit ihnen nicht realisieren. Dazu muss man dann wieder auf eines der anderen Systeme zurück greifen oder auf eine Kreditkarte auf Guthabenbasis.

Einen besonderen Weg geht die Sofortüberweisung. Diesem Veranstalter übergibt man einfach die Zugangsdaten zu seinem Onlinekonto samt PIN und TAN und er wickelt damit eine für den Partner sichere Überweisung ab. Ein noch besserer Hilfsdienst für das Phishing ist kaum denkbar.

Die Bezahlsysteme auf dem grauen Markt kämpfen vor allem mit fünf Problemen:

Transaktionssicherheit: Schnelle Verrechnung und Verfügbarkeit von Valuten. Führend sind dabei die geschlossenen Verrechnungssysteme, die klassische Kontokorrentkonten für angemeldete Kunden anbieten, und Treuhandsysteme wie PaysafeCard und ukash, die digitale Bezugsscheine herausgeben.

Valutierung: Transaktionen zum Verrechnungssystem und Realisierung des Zugangs. Die Speisung bei den nicht mehr relevanten Edelmetall-Verrechnungssysteme ging einfach per Western Union oder ganz normalen Zahlungssystemen. Nur die Auszahlung war kompliziert, weil sie über nationale Edelmetall-Händler erfolgte, die nicht nur rar waren, sondern auch ihren eigenen Schnitt machen wollten. Dank der jetzt üblichen Kreditkarte auf Guthabenbasis ist das kein Problem mehr. Die Herausgeber verdienen gut an den Gebühren, aber die Täter ziehen die Beute aus dem Geldautomaten um die Ecke.

Stabilität: Bei Casinos und proprietären Währungen in Online-Spielen oder virtuellen Welten gibt es keine Bestandssicherheit für Einlagen. Die Bezahlsysteme haben es einfacher, weil sie sich auf die Transaktionen und ihre Marge konzentrieren. Sie tragen kein Risiko wegen der Transaktionssicherheit. Nur die Vorwürfe der Geldwäsche und der Unterstützung krimineller Aktivitäten können sie ernsthaft in Schwierigkeiten bringen. Deshalb wählen sie die geeigneten Standorte im Offshore.

Verkehrssicherheit: Treuhandfunktionen bieten PayPal und zum Beispiel WebMoney und PaysafeCard, weil sich ihre Transaktionen mit einem Kennwort schützen lassen. Nur wer es kennt, kann auch den Erlös erlösen. Daraus folgt das fünfte Problem:

Verfolgbarkeit: Die grauen Systeme pflegen Anonymität und ihre Kunden schätzen das. Wenn sie bemakelte (unversteuerte) Gewinne und kriminelle Beute sichern wollen, dann sind wucherische Gebühren und die Gefahr des Totalverlustes (unangenehm, aber) akzeptabel.

Zunächst war es der Bezahldienst Western Union, der für alle möglichen kriminellen Beutesicherun-

gen missbraucht wurde. Seine Gebühren bei 7,5 % des Umsatzes machten nichts aus, weil es um Beute ging.

In den letzten Jahren entstanden immer mehr kreative Transfersysteme mit Schnittstellen zum normalen Zahlungsverkehr. Die Kreditkarte auf Guthabenbasis ist das beste Beispiel dafür: Master als globales Verrechnungssystem auf Institutsebene hat sich darauf eingelassen und überhaupt nicht gemerkt, welchen Sprengstoff das Geschäftsmodell birgt. Über kurz oder lang kann Master denselben Imageverlust erleiden wie Western Union.

Vouchers von ▸ PaysafeCard und ▸ ukash haben dieselbe Qualität. Sie sind Wertpapiere, die ihre Sicherheitsmerkmale nicht körperlich tragen, sondern durch digitale Codes sichern. Sie sind global verfüg- und unkontrollierbar. Das verspricht kurzfristig gute Gewinne und langfristig schwere Regulierung.

Einfache Lösungen für die Transaktionssicherheit, Valutierung und Treuhandmechanismen sind für den Leistungsaustausch im Internet nötig und von der Finanzwirtschaft zu spät entwickelt worden. In die Bresche sind PayPal und mit mäßigem Erfolg ▸ ClickandBuy gesprungen.

Vouchers und andere unregulierte Bezahlsysteme beweisen, dass ein Markt für anonyme und globale Verrechnungs- und Auszahlungssysteme besteht, die auch ein gefundenes Fressen für die Beutesicherung und Geldwäsche der Cybercrime sind. Das beweisen nicht zuletzt die innovativen Angebote, die bevorzugt in Carder-Kreisen angeboten werden und Transfers zwischen den verschiedenen Bezahlsystemen ermöglichen [349]. Sie können auch mit unattraktiven Gebühren bestehen, weil sie nur die Beute schmälern, nicht aber gefährden. Um sie zu erlangen müssen die Täter nur noch zum nächsten Geldautomaten einer normalen Bank gehen.

Ein Bezahlsystem funktioniert im Internet überhaupt nicht und das ist die Hawala [350]. Dieses der Anweisung (§§ 783 ff. BGB) vergleichbare Rechtsinstitut aus dem arabischen Kulturkreis beruht auf gegenseitigem Vertrauen, zumindest der Hawalare untereinander. Bei diesem schon im Mittelalter entstandenen System wird kein Geld bewegt. Der Geldgeber (Anweisende) beauftragt vielmehr einen Hawalar (Angewiesener) damit, einen bestimmten Geldbetrag an eine andere Person zu zahlen (Anweisungsempfänger). Das macht der Hawalar aber nicht selber, sondern beauftragt damit einen weiteren Hawalar, der sich in der Nähe des Anweisungsempfängers befindet. Tatsächlich zahlt der zweite Hawalar den Anweisungsbetrag aus eigenem Vermögen aus. Später verrechnen die Hawalare untereinander die gegenseitigen Forderungen und gleichen sie aus [351].

Die Hawala ist ein Bezahlsystem außerhalb der volkswirtschaftlichen Gesamtrechnung und der beaufsichtigten Finanzwirtschaft. Als solche ist sie nicht strafbar. Es handelt sich aber um ein Bankgeschäft im Sinne von § 1 Abs. 1 Nr. 1 KWG, das, wenn es gewerbsmäßig betrieben wird, einer Erlaubnis der Bundesanstalt für Finanzdienstleistungsaufsicht bedarf (§ 32 Abs. 1 S. 1 KWG). Der unerlaubte gewerbsmäßige Betrieb von Bankgeschäften ist dann strafbar nach § 54 Abs. 1 Nr. 2 KWG.

Das System der Hawala funktioniert nur auf der Grundlage einer gewachsenen Kultur und einem traditionell untermauertem Vertrauen in die Integrität zu den Hawalaren und insbesondere der Hawalare untereinander. Das gibt es nicht im Internet.

---

[349] **CF**, Konvergenz auf dem Schwarzmarkt, 25.11.2010

[350] **CF**, Anweisung, Überweisung, Hawala, 2007

[351] In der Finanzwirtschaft und beim Roaming der Mobilfunk-Provider nennt man das „Clearing“.

2.8.3 Bitcoins

Bitcoins - BTC - sind digitale und gleichzeitig anonyme Werteinheiten, die stark verschlüsselt sind und in einem offenen Peer-to-Peer-Netzwerk gegen andere Dienste und Leistungen getauscht werden können. Sie lassen sich als Dateien mit asymmetrischer Verschlüsselung nicht beliebig, sondern nur durch besonders hohe Rechenleistung erzeugen [352], die, je mehr BTC bereits erzeugt sind, immer höher wird. Dadurch ist die Gesamt-BTC-Menge rechnerisch auf 6.929.999 Blocks und somit auf knapp 21 Millionen BTC begrenzt [353].

Bitcoins haben keine materielle (Edelmetall) oder abstrakte Wertbasis (geldwirtschaftliche Systeme unter volkswirtschaftlicher Absicherung), können nur durch dem Einsatz immer höherer Rechenleistungen erzeugt werden und bilden ihren Tauschwert durch schlichte Marktmechanismen, also Akzeptanz, Angebot und Nachfrage. Die aktuelle "Geldmenge" umfasst etwa 6,4 Millionen BTC [354]. Ihr Tauschwert pro Einheit liegt gegenwärtig bei etwa 19 US-$, so dass der BTC-Geldmarkt zur Zeit auf etwa 122 Millionen US-$ beschränkt ist [355]. Alle 10 Minuten kann (statistisch) ein neuer "Block" errechnet werden [356].

Bereits jetzt sind die BTC stark überbewertet. Sie sind zunächst 1:1 an der €-Währung ausgerichtet gewesen [357] und lassen ganz erhebliche Wechselkursschwankungen erwarten. Ihr System beruht auf einer normativen Mengengrenze, die nur auf einer mathematischen und veränderlichen Variablen fußt. Geldwirtschaftliche Kontrollinstrumente und eine Regulierung fehlen. Ihr Tauschwert wird allein vom Markt bestimmt. Nicht zuletzt deshalb warnt der Bundesverband Digitale Wirtschaft - BVDW - vor Bitcoins als Zahlungsmittel [358].

Ein bislang einzelnes Beispiel belegt, dass das Transfersystem nicht vor Diebstahl schützt [359]: *Ein Benutzer, der sich als Early Adopter bezeichnet, behauptet, ihm seien über Nacht etwa 25.000 Bitcoins (aktueller Wert rund 500.000 US-Dollar) gestohlen worden.* Die Bitcoin-Tauschbörse Mt. Gox wurde anschließend wegen ihrer Sicherheitsmängel geschlossen [360].

Ein anderer Trojaner nutzt die Rechenkapazitäten eines Botnetzes, um die schwierigen kryptographischen Rätsel zu knacken, die mit der Errechnung neuer Coins verbunden sind [361]. Die Cybercrime-Szene ist eben erfinderisch, wenn irgendwo Geld lockt.

Die Warnungen des BVDW sind deshalb nicht unberechtigt, zwar nicht, weil ein gesetzgeberisches Verbot oder der Niedergang der offiziellen Micropaymentsysteme droht, sondern weil undurchsichtige und meistens irrational gesteuerte Marktsysteme zur Instabilität und zu starken Schwankungen neigen. Die an lockeren Leinen regulierten Börsen-, Wertpapier- und Kapitalmärkte haben das längst bewiesen.

Kommentatoren wie Mühlbauer heben hingegen die Anonymität des Systems hervor, das keine Rückabwicklung erfolgloser Zahlungen zu- und steuerliche Schätzungen erwarten lässt [362]. Der Weg-ist-weg-Einwand erinnert mich an die konsequente russische Herangehensweise, die auch WebMoney zugrunde liegt: Mach Dein Geschäft!

---

352 Bitcoin

353 Wie lange wird es dauern bis alle Münzen generiert sind?

354 Was ist die aktuelle Gesamtzahl an existierenden Bitcoins?

355 Mt. Gox (USD/Liberty Reserve) [Grafik]

356 Warum muss ich zehn Minuten warten, bevor ich Geld ausgeben kann, das ich bekommen habe?

357 Wie lange wird es dauern bis alle Münzen generiert sind?

358 BVDW warnt Verbraucher und Händler vor Bitcoins als Zahlungsmittel, BVDW 01.06.2011

359 Florian **Hofmann**, Bitcoin-Diebstahl: Eine halbe Million US-Dollar weg? Heise online 15.06.2011; Trojaner stiehlt virtuelle Währung, Heise online 17.06.2011.

360 Bitcoin-Tauschbörse nach Angriff geschlossen, Heise online 20.06.2011

361 Twitter-gesteuertes Botnetz schöpft BitCoins, Heise online 04.08.2011

362 Peter **Mühlbauer**, Digicash 2.0, Telepolis 06.06.2011

Ich kriege meinen Anteil! Und dann ist Ruhe!

Allenfalls an den Schnittstellen, an denen Bitcoins in andere Werteinheiten umgetauscht werden, können die Inhaber identifiziert werden [363].

Das Ergebnis ist ernüchternd: Die BTC sind ein ernsthaftes Zahlungsmittel nur für Internetkriminelle oder Spekulanten, die schwere Kursverluste schmerzfrei verkraften können. Dass sich Finanzinstitute als Wechselstuben zur Verfügung stellen, ist unverantwortlich und unverständlich genug. Vielleicht lockt einfach nur der schnelle Gewinn, möchte der Böswillige meinen.

2.8.4 Fazit

Anonymität ist das Schlagwort, das den grauen Bezahlsystemen zugrunde liegt und das nicht ohne Recht. Sie ist auch die Grundlage von Währungen, die auf der Basis von Wertpapieren und staatlich garantierten Tauschfunktionen wirtschaftliche Prozesse im Gang halten.

Anonymität in der Tauschwirtschaft und Rechtsstaat sind Staatsziele, die sich nicht ausschließen, aber kräftig aneinander reiben. Der Rechtsstaat braucht die Größe, über Subsistenzwirtschaft im privaten Rahmen und persönliche Allüren oder kleine Schweinereien hinwegzusehen, und den Mut, Grenzen zu setzen, wenn er oder wesentliche persönliche Interessen erheblich bedroht sind. Deshalb ist das Micropayment als solches und seine Anonymität überhaupt kein Problem, sondern erst dann, wenn es als Instrument zur Beschaffung von Vermögenswerten in einer Größenordnug genutzt wird, um auf kriminelle Art den Lebensunterhalt (mindestens) anzureichern oder den richtigen Reibach zu machen. Wenn es dazu kommt, sind Geldwäscheregularien, Mitteilungspflichten, die Öffnung der Anonymität und vernünftige Regeln zur Verhinderung und zur Strafverfolgung zwingend geboten.

Das BVerfG hat deshalb – nur zum Beispiel – nicht die Vorratsdatenspeicherung als solche verboten, sondern die unzureichenden Verwertungs-, Aufbewahrungs- und Zugriffsregeln angeprangert [364]. Die darin zum Ausdruck kommende Differenzierung tut auch der Bewertung der Bezahlsysteme gut. Sie erfordern einen beachtlichen wirtschaftlichen Aufwand und müssen sich für die Betreiber lohnen. Das ist nur dann der Fall, wenn genug Kunden für sie gewonnen werden können. Western Union lehrt den Umkehrschluss: Das Image ist nachhaltig belastet, wenn die Missbrauchskontrolle fehlt und sich der regelmäßige Missbrauch im öffentlichen Bewusstsein verfestigt. Das Gegenbeispiel dazu ist eBay, wo nachhaltige Kontrollroutinen laufen und Warnhinweise dem Kunden gemeldet werden.

---

[363] Florian **Hofmann**, Bitcoin-Diebstahl: Eine halbe Million US-Dollar weg? Heise online 15.06.2011;

[364] **BVerfG**, Beschluss vom 22.04.2009 - 1 BvR 256/08

Die Internetwirtschaft betritt Neuland, ist eher geneigt, den großen und vor allem schnellen Profit zu erzielen, und weniger geneigt dazu, im Rahmen einer langfristigen Strategie eigene Marktanteile strategisch zu sichern.

Das kann sich rächen, wie das Beispiel PaySafeCard zeigt: Am 18.02.2010 änderte das Unternehmen die Systemeinstellungen und ließ die nachträgliche Änderung des Kennworts für den digitalen Bezugsscheins nicht mehr zu. Dadurch verlor das Bezahlsystem seine Funktion als offenes Bezahlsystem für die Cybercrime-Szene. Sie vertraute darauf, dass der Käufer die PSC- und die PIN übermittelt und der Verkäufer sich die PSC durch die Änderung der PIN im Onlineverfahren sichert. Nun verlangte PaySafeCard die Legitimation mit einem ausgedruckten Bon [365].

Die Cybercrime-Szene reagierte empört und rief zum DDoS-Angriff gegen PSC auf [366]. Es kam zu längeren Ausfallzeiten (Downtime) der PSC-Homepage, wobei jedoch nicht bekannt ist, ob es schlussendlich durch die Angriffe begründet war, oder durch Wartungsarbeiten, wie offiziell verlautbart wurde. Nur einen Tag nach den DDoS-Aufrufen, am 19.02.2010, revidierte der Bezahldienstleister seine neue Passwortpolitik. Zum 22.02.2010 sollte eine Einrichtung und Änderung eines Passworts auch wieder ohne die Einsendung des Kassenbons möglich werden. Das wurde von der Szene freudig begrüßt.

---

[365] **CF**, DDoS gegen PaySafeCard, 23.05.2010

[366] Marc-Aurél **Ester**, Ralf **Benzmüller**, Whitepaper 04/2010. Underground Economy - Update 04/2010, G Data 22.04.2010, S. 6 bis 8

2.9 Organisierte IuK-Kriminalität

Von den organisierten Internetverbrechern wurde erstmals in McAfee's Zweiter großen europäischen Studie über das Organisierte Verbrechen und das Internet [367] vom Dezember 2006 gesprochen. Über ihre Formen und Besonderheiten habe ich ausführlich 2010 berichtet [368]. An dieser Stelle beschränke ich mich deshalb auf die wesentlichen Aspekte der Erscheinungsformen und werfe einen allgemeinen Blick auf die einschlägigen Strafvorschriften, die wegen der Besonderheiten im Einzelfall variieren können, wie schon die aufgeführten Fallbeispiele gezeigt haben.

2.9.1 Malware-Fabriken

Paget berichtete 2010 davon, dass infolge von Wirtschaftskrisen seit 1990 „Virus-Fabriken“ in Bulgarien und seit 1998 in Russland entstanden [369]. Danach sollen Solntsevskaya und Dolgopruadnanskaya die zwei größten Mafia-Organisationen in Russland sein, die sich der Internetkriminalität widmen und jährlich 25 Prozent der Absolventen der russischen Wissenschafts- und Technologie-Studiengänge einen Job bieten sollen [370]. Über das Innenleben dieser Organisationen und ihre Geschäftsfelder erfahren wir nicht mehr.

Schon 2008 berichtete Balduan über cyberkriminelle Projektmanager (Independent Business Man, Koordinator [371]) und Operation Groups: *Die zentrale Figur jedoch ist ... ein „Independent Business Man“ – eine Person, die Kontakte zur Unterwelt pflegt und zwischen Bot-Herdern, Hackern, Malware-Schreibern und Spammern koordiniert. ... mithilfe der Botnetz-Infrastruktur kann der Koordinator Unternehmen mit verteilten Massenangriffen auf ihre Webseiten drohen und so Schutzgeld erpressen, Spam-Wellen mit Werbung für überteuerte Produkte oder Aktien lostreten oder tausendfach persönliche Informationen wie Bankzugangsdaten ergaunern.*

Die ***arbeitsteilige Cybercrime*** ist die vom Gewinnstreben bestimmte planmäßige Begehung von IT-Straftaten, die einzeln oder in ihrer Gesamtheit von erheblicher Bedeutung sind. Ihre planenden Täter greifen dazu auf etablierte Strukturen (wie Botnetze und Rogue-Provider) und Gruppen mit Spezialisten (Operation Groups) zurück, deren Dienste und Handlungen sie zur Erreichung des kriminellen Zieles zusammenführen.

Die ***Organisierte Cybercrime*** ist die vom Gewinn- oder Machtstreben bestimmte planmäßige Begehung von IT-Straftaten, die einzeln oder in ihrer Gesamtheit von erheblicher Bedeutung sind, wenn mehr als zwei Beteiligte auf längere oder unbestimmte Dauer arbeitsteilig

a. unter Verwendung gewerblicher oder geschäftsähnlicher Strukturen,

b. unter Anwendung von Gewalt oder anderer zur Einschüchterung geeigneter Mittel oder

c. unter Einflussnahme auf Politik, Medien, öffentliche Verwaltung, Justiz oder Wirtschaft zusammenwirken.

CF, neue Definition der Cybercrime, 27.08.2008

Seine Subunternehmer seien die Operation Groups [372]. Sie bilden kleine Gruppen und spezialisieren sich unter der Leitung eines führenden Kopfes auf bestimmte Dienstleistungen. Beispiele dafür sieht Balduan in der Herstellung von Malware und in der Zulieferung von Exploits und Rootkits. Insoweit sieht Balduan getrennte Gruppen im Einsatz und nicht etwa gefestigte, einheitliche Strukturen. Das würde zu dem Bild passen, das wir von schwarmähnlichen Strukturen bei der Kommunikation und Zusammenarbeit kennen (◗ Kasten oben).

Auch von ihrer Arbeitsweise her ist im Zusammenhang mit der Programmierung professioneller Mal-

[367] Zweite große europäische Studie über das Organisierte Verbrechen und das Internet, McAfee Dezember 2006 (seit der Umstellung des Webangebots im Dezember 2010 nicht mehr verfügbar).

Einzelheiten bei: **CF**, globale Sicherheitsbedrohungen. Cybercrime, 27.07.2008.

[368] Dieter **Kochheim**, Cybercrime, 24.06.2010 [C.1 Schurken-Provider und organisierte Cybercrime]

[369] Dieter **Kochheim**, Cybercrime und politisch motiviertes Hacking, 20.10.2010, S. 4, 5.

[370] Ebenda, S. 6.

[371] Gordon Bolduan, Digitaler Untergrund, Technology Review 4/2008, S. 26 ff.
Einzelheiten: **CF**, Koordinatoren, 13.07.2008.

[372] Ebenda.

ware eher von kleineren Teams auszugehen, die die Software im Rahmen eines Projektplans arbeitsteilig, mit definierten Meilensteinen und Zulieferungen (kritische Kette) erstellen. Insoweit erscheint es schlüssig, dass sich um die Akquise und die kaufmännische Abwicklung der Leiter einer Operation Group kümmert.

Auf die Herstellung von Malware sprechen vor allem §§ 202c Abs. 1 Nr. 2, 263a Abs. 3, 303a Abs. 3 und 303b Abs. 5 StGB an, die mit Freiheitsstrafen bis zu einem oder drei Jahren drohen (▸ Vorbereitungshandlungen).

§ 129 StGB macht keinen Unterschied wegen der Straftaten, zu deren fortdauernden Begehung sich eine ▸ kriminelle Vereinigung bildet. Das Beispiel vom ▸ Internetradio zeigt, dass der BGH keine Bedenken dagegen erhebt, auf die kriminelle Vereinigung auch Ausführungstaten aus dem Bereich der mittleren (Volksverhetzung, § 130 StGB) oder der einfachen Kriminalität anzuwenden (Verbreitung von Propagandamitteln und Verwendung von Kennzeichen verfassungswidriger Organisationen, §§ 86, 86a StGB; Gewaltdarstellung, § 131 StGB). Die einzigen tatsächlichen Grenzen bestehen darin, dass sich mindestens drei Täter vereinigen müssen und dass der zentrale Zweck der Vereinigung die auf Dauer angelegte Begehung von Straftaten ist.

Auf eine Operation Group übertragen, die das Ziel verfolgt, Malware herzustellen, bedeutet das, dass sich mindestens zwei Programmierer und ein Leiter der Gruppe dauerhaft verbunden haben müssen, um eine kriminelle Vereinigung zu bilden. Dem Leiter droht womöglich als Rädelsführer eine Mindeststrafe von sechs Monaten Freiheitsstrafe (§ 129 Abs. 4, 1. Halbsatz StGB) [373].

Das bedeutet, dass bereits der Zusammenschluss weniger Programmierer unter einer kaufmännischen Leitung trotz leichter krimineller Ausführungstaten eine nachhaltige Strafverfolgung als kriminelle Vereinigung unter Einsatz operativer Ermittlungsmethoden eröffnet. Dazu bedarf es nicht erst großer „Virus-Fabriken“, die sich der industriellen Produktion von Malware widmen, sondern reichen kleine Verbünde aus (Malware-Manufakturen).

[373] Die Strafdrohung im Grunddelikt mit einer Höchstfreiheitsstrafe von 5 Jahren lässt die Mitgliedschaft in einer kriminellen Vereinigung als Straftat im mittleren Schwerebereich erscheinen. Im Zusammenhang mit der Überwachung der Telekommunikation hat der Gesetzgeber das Delikt zu den besonders schweren zugeordnet: § 100a Abs. 2 Nr. 1 d) StPO.

2.9.2 globale Botnetze

Dank Malware-Baukästen ist das zunehmende Entstehen von kleineren ▸ Botnetzen zu erwarten. Aufgrund ihrer einfacheren „Strickweise“ dürften sie jedoch für die künftigen Antiviren- und Sicherheitsprogramme keine nennenswerten Schwierigkeiten bereiten.

Das sieht anders aus bei den etwa zwei Dutzend richtig großen, globalen Botnetzen, die gewerbsmäßig genutzt werden. Nach Paget sind für ihren ständigen Betrieb zwei bis drei Programmierer nötig sowie ein oder zwei Leute, die sich um die kaufmännische Abwicklung kümmern.

Der Betrieb eines Botnetzes setzt die erfolgreiche Installation von Botware voraus, die die angegriffenen Computer zu Zombies macht. Bereits bei der Installation der Botware machen sich die Verbreiter wegen des ▸ Ausspähens von Daten und wegen ▸ Computersabotage strafbar (§§ 202a Abs. 1, 303b Abs. 1 Nr. 2. StGB). Der besonders schwere Fall der schweren Computersabotage (§ 303b Abs. 4 in Verbindung mit Abs. 2 StGB) droht immerhin mit Freiheitsstrafen bis zu zehn Jahren. Das ist der Fall, wenn gewerblich genutzte PCs zu Zombies werden (schwere Computersabotage) und darüber hinaus die Täter gewerbs- oder bandenmäßig handeln. Diese nachhaltige Strafbarkeit tritt bereits beim Aufbau eines großen Botnetzes ein, ohne dass es zum Spam- oder Malwareversand, zum DDoS-Angriff, zur Verbreitung illegaler Inhalte oder zum verteilten Rechnen kommen muss [374].

Wie bei den ▸ Malware-Manufakturen kommt auch im Zusammenhang mit dem Aufbau eines Botnetzes die Bildung einer kriminellen Vereinigung in Betracht (§ 129 StGB), wenn sich mindestens drei Gründungsmitglieder zusammen tun. Sie findet ihre dauerhafte Fortsetzung im Betrieb des Botnetzes. Mit Ausnahme der Verbreitung von ▸ Spam-Nachrichten, die wegen des Einzelfalls betrachtet werden müssen, unterliegen alle üblichen Botnetz-Aktionen einer eigenen Strafbarkeit (▸ Malware in Aktion). Die Probleme der ▸ Klammerwirkung und der einzelnen materiellen Taten muss im Zusammenhang mit dem Handeln einer kriminellen Vereinigung müssen weniger an den Ausführungstaten (krimineller Einsatz des Botnetzes) als an den Förderungshandlungen in Bezug auf den kriminellen Gesamtplan orientiert werden. Beim Botnetz sind das vor allem die Aktionen, die der Ausdehnung, also der Gewinnung neuer Zombies, oder dem Update auf neue Programmversionen dienen.

Für die Botnetze kann deshalb keine einheitliche Linie vorgeschlagen werden. Die Einzeltäter, die zum Beispiel Botnetze mit Hilfe eines Malware-Baukastens aufbauen, unterliegen dabei bereits den einfachen Strafdrohungen aus den §§ 202a Abs. 1, 303b Abs. 1 Nr. 2. StGB. Hier ist auch zu fragen, mit welchem Ziel der Täter das Botnetz aufbaut. Wenn er sich auf DDoS-Angriffe ohne Erpressungen beschränken will, handelt er nicht gewerbsmäßig im Sinne der besonders schweren Form der schweren Computersabotage.

Handelt es sich um Tätergruppen mit drei und mehr Leuten, dann kommt bereits im Aufbaustadium ein besonders schwerer Fall der schweren Computersabotage und die Gründung einer kriminellen Vereinigung in Betracht.

Während beim Einzeltäter wegen der Ausführungstaten auf jede einzelne Tat abzustellen ist, sind bei der kriminellen Vereinigung eher die Förderungshandlungen zu betrachten, die in der Rekrutierung neuer Zombies und im Update der Botware zu sehen sind.

Im Einzelfall sind somit viele Weichenstellungen zu beachten. In keinem Fall jedoch ist der Aufbau und der Betrieb eines Botnetzes straflos [375].

---

[374] Die Computersabotage erfüllt zwar beim besonders schweren Fall der schweren Computersabotage die formellen Voraussetzungen für eine schwere Straftat. In den ▸ Straftatenkatalog des § 100a Abs. 2 StPO wurde sie aber nicht aufgenommen.

[375] Ausnahme: Einrichtung in einer kontrollierten Testumgebung unter Zustimmung der Beteiligten.

2.9.3 Schurkenprovider

Schurken-Provider betreiben wie andere Anbieter im Internet auch eine normale technische Infrastruktur. Sie sind autonome Systeme, also in sich geschlossene technische Netzwerke, die mit anderen internationalen Netzen und Carriern durch Verträge verbunden sind [376]. Ihre Netzdienste sind dieselben, die auch andere Host- und Zugangsprovider bieten: Die Verwaltung von DNS-Adressen, Speicherplatz (Hostspeicher) und Kommunikationsplattformen (Chat, geschlossene Benutzergruppen).

Sie unterscheiden sich hingegen wegen ihres Geschäftsmodells, weil sie ihre Kunden gegenüber der Öffentlichkeit und vor allem vor den Strafverfolgungsbehörden abschotten. Dazu werden Scheinfirmen eingerichtet, die als Inhaber von Domänen geführt werden, oder Fantasie- und Aliasnamen benutzt. Dort, wo sich schurkische Dienste in der Öffentlichkeit präsentieren, wird dadurch ausgeschlossen, dass die Betreiber und Hinterleute aus Registern oder anderen öffentlichen Quellen identifiziert werden können (Bullet Proof Domains [377]).

Beispiel gebend, aber kein Einzelfall, ist das in St. Petersburg ansässig gewesene Unternehmen Russian Business Network – RBN [378]. Über die Hinterleute dieses Unternehmens sind viele Spekulationen im Umlauf und Faber hat in der c't die Fakten bemerkenswert zusammen getragen und bewertet [379]. Ungeachtet der technischen Fragen kann ein Schurkenprovider [380] nur dann längerfristig bestehen, wenn er in sein soziales und wirtschaftliches Umfeld eingebunden ist und sein Handeln gefördert oder zumindest toleriert wird. Er ist darauf angewiesen, die Netzleistungen großer und leistungsstarker Zugangsprovider und Carrier zu nutzen und kann sich deshalb nur mit besonderen Tricks verstecken, ohne aber dadurch unsichtbar zu werden.

Ester und Benzmüller [381]: *Hier finden alle ein Zuhause, die Drop Zones für die Daten ihrer Botnetze suchen, illegale Shops betreiben, Command & Control (C&C)-Server sicher unterbringen wollen und dergleichen mehr. Unter Dropzones ist in diesem Zusammenhang ein Server zu verstehen, auf dem beispielsweise die auf dem Rechner des Opfers installierte Spyware ihre gesammelten Daten ablegen kann. Das Produktportfolio reicht hier wie bei jedem seriösen Anbieter vom kleinem Webspace-Angebot, über virtuelle Server bis hin zu ganzen Serverclustern, je nach Geldbeutel und Anforderungen.*

2.9.3.1 Organisation und Adressen im Internet

Das Internet verfügt über keine einheitliche technische Struktur, wie wir sie etwa von den Telefonnetzen gewohnt sind, sondern beruht auf der Zusammenarbeit großräumiger Netzbetreiber (Carrier, Anschlussnetzbetreiber) und regionaler Anbieter. Ungeachtet ihrer Größe und Leistungsfähigkeit sind sie jeder für sich ein Autonomes System – AS, das sich zur Durchleitung „fremder“ Daten verpflichtet, um im Gegenzug die eigenen Daten an andere AS zur Weiterleitung zu übergeben. Die aufgenommenen und abgegebenen Datenmengen werden untereinander abgerechnet (Peering) und nur die weltweit größten Carrier, etwa ein Dutzend Unternehmen, haben eine solche Marktstellung, dass sie keinen fremden „Transit“ hinzu kaufen müssen (Tier 1 [382]).

Neben den nummerischen Adressen des Internetprotokolls werden von der Internetverwaltung (In-

[376] **CF**, autonome Systeme und Tiers, 2007

[377] Jürgen **Schmidt**, Hydra der Moderne. Die neuen Tricks der Spammer und Phisher, c't 18/2007; ebenda, ... Bullet Proof Domains.

[378] **CF**, Russian Business Network – RBN, 13.07.2008; Dieter **Kochheim**, Cybercrime, 24.06.2010, S. 80 (Schurken-Provider und organisierte Cybercrime); Dieter **Kochheim**, Netzkommunikation, 10.07.2010, S. 20 (manipulierte Welt).

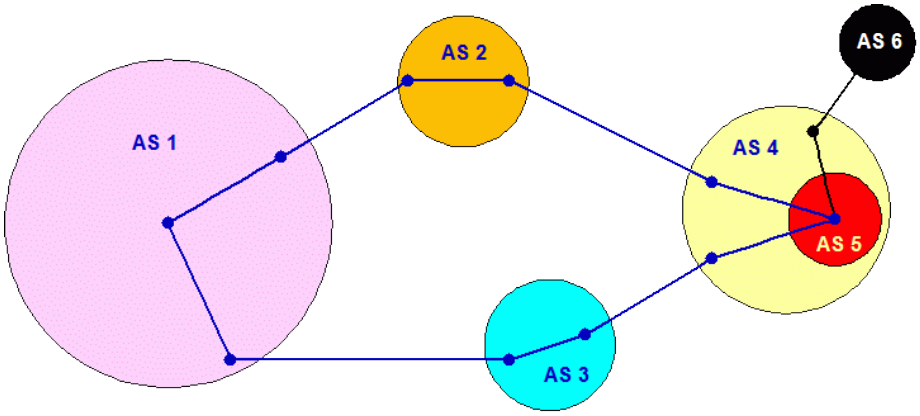
[379] Frank **Faber**, Unter Verdacht. Eine russische Bande professionalisiert das Cybercrime-Business, c't 11/2008, S. 92

[380] Auch „Rogue Provider“ oder „Rogue ISP“.

[381] Marc-Aurél **Ester**, Ralf **Benzmüller**, G Data Whitepaper 2009. Underground Economy, 19.08.2009, S. 10

[382] **CF**, Tier-1 ... 2 ... 3, 2007

Autonome Systeme - AS - verfügen über Verbindungen zu mindestens zwei anderen AS. Im Beispiel sind deshalb zwei Routen möglich, um vom AS 1 zum AS 4 zu gelangen.



Im vorläufigen Ziel, dem AS 4, verbirgt sich das AS 5, wobei es sich um einen einzigen Serverschrank irgendwo im Rechenzentrum von AS 4 handeln kann. Er muss nur über einen Router verfügen, der Signale aufnimmt und wieder weiter leitet, einen Domain Name Server, um Domainnamen zu verwalten, und eine Firewall, mit der sich VPN-Tunnel aufbauen lassen (Virtual Private Network).

AS 4 muss ein üblicher, möglichst unauffälliger Zugangsprovider mit starken Verbindungen zu anderen Carriern sein. Sein Betreiber muss auch bereit sein, seine technische Infrastruktur dem Schurken (AS 5) zur Verfügung zu stellen. Aufgrund der kurzen physikalischen Wege gibt es zwischen AS 4 und AS 5 keine bedeutsamen Signallauf- oder Verarbeitungszeiten. Tatsächlich befinden sie sich in demselben LAN (Local Area Network).

AS 5 ist ein gekapseltes System, das nach außen hin wie ein vollwertiges AS wirkt. Sein DNS-Server erlaubt es ihm, alle möglichen und unsinnigen Meldungen über seinen Standort und seine Identität und die Identität der Kunden, die es hostet, nach außen zu melden (Whois- und DNS-Protection).

Die getarnten Hosting- und sonstigen Serverdienste, die AS 5 anbietet, können am selben physikalischen Standort, also räumlich innerhalb von AS 4 installiert werden. Das hat den Vorteil, dass die Performance nicht leidet, aber den Nachteil, dass AS 5 zu einfach als direktes Anhängsel zum AS 4 gemessen und erkannt werden kann.

Abhilfe schafft zunächst die Firewall im AS 5, die die von außen kommenden Ping-, Tracerouting- und Whois-Anfragen abfängt.

Eine noch bessere Tarnung wird erreicht, wenn AS 5 wie ein Türsteher die Signalvermittlung zu einem weiteren, aber räumlich entfernten Standort vermittelt. Die Verbindungen zwischen AS 5 und AS 6 werden dazu über einen VPN-Tunnel geführt, wobei die Zwischenstationen (Knoten) beim Routing anonym bleiben.

Die Knoten zwischen AS 5 und AS 6 müssen dabei mitspielen, das Tunneln zulassen und genau zwischen AS 5 und AS 6 routen. Das bedeutet, dass nur eine begrenzte Anzahl von Knoten vorhanden sein dürfen. Ihre Betreiber müssen eingeweiht sein, das Treiben von AS 5 akzeptieren und schließlich verlangt die Tunnelstrecke Performance, weil sonst die Kunden unzufrieden sind. Das bedeutet, dass die Tunnelstrecke nicht zu lang sein darf und die Verbindung mit hoher Bandbreite ausgestattet sein muss, weil beides die Signallaufzeit verzögern würde.

Bei dieser Lösung erscheint AS 5 für äußerliche Messungen als harmlose Zwischenstation zu AS 6. Ein Blick auf die AS-Auswertung bei robtex.com zeigt aber, dass AS 6 nur oder fast ausschließlich an AS 5 angeschlossen ist und dass AS 5 fast ausschließlich Datenverkehr mit AS 4 austauscht. Daraus lassen sich sinnvolle Schlüsse ziehen.

ternet Soceity: ICANN, IANA und andere [383]) auch feste Nummern für die Autonomen Systeme vergeben. Das geschieht nicht einzeln sondern blockweise, worauf die Einzelzuweisung durch die regionalen Zonenverwaltungen – RIR – erfolgt, für die europäische Zone also von dem RIPE Network Coordination Centre in Amsterdam. Die AS melden den Zonenverwaltungen, welche anderen AS über sie erreichbar sind. Diese Daten werden in Routingtabellen aufgenommen, auf die die Verbindungsnetze nach Maßgabe des Border Gateway Protocol – BGP [384] - zugreifen, um die von ihnen transportierten Daten weiter zu geben.

Die Verantwortung für die Meldungen zum BGP tragen die Betreiber der AS selber, ohne dass eine strikte Kontrolle oder Prüfung erfolgt.

Im Prinzip dasselbe gilt für die Verwaltung der beschreibenden Internetadressen (Domain Name Service – DNS). Die zentrale Internetverwaltung beschränkt sich auf die Verwaltung der Namensräume für die generischen (.com, .net und andere)

[383] Dieter **Kochheim**, Verwaltung von Nummern und Namen im Internet, 17.07.2010

[384] **CF**, böswillige BGP-Manipulationen, 10.07.2010

und Länderdomänen (.de, .ru uvam), deren Verwaltung ebenfalls an die Zonenverwaltungen abgegeben ist. Die Vergabe der einzelnen Second Level Domains – SLD (zum Beispiel cyberfahnder.de) – ist in aller Regel an eine nationale Vergabestelle übertragen, so in Deutschland an die DeNIC (Deutsches Network Information Center). Sie betreiben auch die Datenbanken, mit deren Einträgen die beschreibenden Namen aufgelöst und Whois-Abfragen beantwortet werden.

Die Einträge und Änderungen in den Whois-Datenbanken beruhen auf den Meldungen der Registrare, also von den Einrichtungen, die zur Vergabe von Namen im einzelnen berechtigt sind. Wenn das AS einen eigenen DNS-Server betreibt, um eigene Domainnamen selbständig zu verwalten, verweisen die zentralen Namensverwaltungen auf den regionalen DNS-Server für das Routing im einzelnen. Das AS hat es damit in der Hand, den Inhalt aller Meldungen über einen Domänennamen zu kontrollieren und zu bestimmen.

2.9.3.2 Dienste eines Schurkenproviders

Das Kerngeschäft des RBN und anderer Schurkenprovider besteht darin, ihren zahlenden Kunden für ihre heiklen oder kriminellen Aktivitäten Abschottung, also einen "sicheren Hafen" zu bieten. Das verlangt nach

▷ anonymisierten Speicherstandorten,

▷ einer anonymisierten Adressverwaltung (Maskierung von DNS-Eintragungen),

▷ komfortablen Anbindungen an das Internet und

▷ einer Niederlassung, in der der Schurkenprovider ohne Angst vor Repressalien handeln kann.

Die ersten Voraussetzungen dafür sind, dass der Schurke ein eigenes Rechenzentrum einrichtet und sich – möglichst über einen unauffälligen und etablierten Partner – eine oder mehrere AS-Nummern beschafft. Diesen Partner oder andere leistungsfähige Carrier braucht der Schurke auch, um sein AS in das AS-Netz des Internets einzubinden und seine AS-Adressse an die Namensverwaltung zu melden. Schließlich muss der Schurke auch seinen Kunden schnelle und breitbandige Verbindungen bieten, weil sie sonst bald wieder abspringen würden. Auch dazu bedarf es leistungsstarker und unauffälliger Partner.

Um seine Aktivitäten zu tarnen, sollte das AS nur als Durchlaufstation erscheinen und für die heiklen Webdienste der Kunden den Transfer zu weiteren AS vermitteln, die am selben Ort betrieben werden können (siehe Schaubild auf der Vorseite). Sobald der Datenverkehr das schurkische AS durchläuft, hat sein Betreiber alle Meldungen über Standorte, Inhaber und Adressen in seiner Hand und kann sie beliebig manipulieren.

Das AS ist berechtigt, eine eigene Adressenverwaltung durchzuführen. Dahinter verbirgt sich nichts anderes als ein DNS-Server, der dazu da ist, für eine beschreibende Internetadresse den physikalischen Standort anhand der nummerischen Adresse des Internetprotokolls zu melden. Darüber hinaus liefert der DNS-Server die persönlichen Angaben über den Inhaber der DNS-Adresse. Damit verfügt jedes AS über ein

mächtiges Werkzeug. Mit seinem DNS-Server kann es die gespeicherten Domänennamen zu jedem beliebigen physikalischen Standort leiten und in der Datenbank im Übrigen jeden Unfug über den Inhaber melden.

In Fachkreisen wird das als "Whois Protection" bezeichnet. Es ist nichts anderes als die Verschleierung der Betreiberdaten, um ihn vor den Nachstellungen der Strafverfolgung oder von Abmahnern zu schützen. In offenen Foren findet man dazu euphorische Lobhudeleien: Endlich keine Abmahnungen und teure Anwaltsforderungen mehr!

Das zweite mächtige Werkzeug, das dem AS zur Verfügung steht, ist die Anonymisierung von Servern.

Mit dem einfachen Kommando "Ping" lässt sich die technische Erreichbarkeit einer Netzadresse überprüfen. An ihr kann sich ein Netzknoten befinden (Router, Switch, Gateway) oder ein Endgerät, das Dateien (Hostspeicher, FTP) oder Datendienste (Webserver, Datenbanken) birgt. Auf das Ping-Kommando meldet das angeschlossene Gerät seine Identität. Das AS kann alle Rückmeldungen unterbinden, wenn es an seinen Eingängen Firewalls betreibt, die die Meldungen nicht durchlassen. Es kann auch genau vorgeben, was die Firewalls an die Gegenstellen senden. Das kann jeder Quatsch sein.

Vom Grundgedanken her haben die ersten Ziffern der nummerischen IP-Adressen eine weiträumige geographische Zuordnung. Das gilt aber nur, solange sie blockweise von der Internetverwaltung vergeben werden. Einzelne IP-Adressen oder „kleine Blöcke“ werden gehandelt und können beliebig in das Subsystem eines AS eingebunden werden. Das ermöglicht es dem Schurkenprovider, weltweit verteilte Standorte vorzugaukeln.

Die wesentliche Aufgabe eines Schurkenproviders ist die der Schnittstelle zum Internet als solches. Die heiklen Dienste der Kunden kann er auf andere Standorte verlagern und dazu auch die Zombies in einem Botnetz zum verteilten Hosting (Speicher) missbrauchen. Eine stabile Erreichbarkeit kann unter Verwendung der Fast Flux-Technik erzielt werden, mit der die nummerischen IP-Adressen einer Endanwendung ständig verändert werden.

Neben den technischen Maßnahmen zur Tarnung muss der Schurkenprovider sich selber abschotten, so dass er nicht gezwungen werden kann, Auskünfte über seine Kunden zu geben (Beschwerderesistenz). Das ist am einfachsten, wenn er nichts weiter über seine Kunden weiß als das, dass sie pünktlich und regelmäßig zahlen. Für das RBN hat gegolten, dass die Kunden umso mehr zahlen mussten, je häufiger Beschwerden oder Anfragen erfolgten.

Auch die Identifikation über die Zahlungswege wird erschwert, wenn Banken an exotischen Standorten oder ▸ graue Bezahlsysteme genutzt werden.

2.9.3.3 Strafbarkeit

Eine an den organisatorischen Maßnahmen des Schurkenproviders ausgerichtete Strafbarkeit besteht nicht. Er greift nicht aktiv in die Rechte anderer ein, späht deren Daten nicht aus, fängt sie auch nicht ab, und sabotiert nicht deren Computer. Das gilt auch für das Whois Protection und die Serveranonymisierung im Hinblick auf die Fälschung beweiserheblicher Daten (§ 269 Abs. 1 StGB): Er nimmt keinen Einfluss auf fremde Datenverwaltungen, sondern nur auf die eigene Infrastruktur, so dass er nur straflos lügt, aber nicht beweiserhebliche Erklärungen anderer fälscht.

Dasselbe gilt für die Mittelbare Falschbeurkundung (§ 271 StGB), die mit Freiheitsstrafe bis zu drei Jahren dem droht, der Tatsachen über erhebliche Rechtsverhältnisse wahrheitswidrig in öffentlichen Dateien oder Registern speichert oder darauf hinwirkt. Dieser Beurkundung muss eine öffentliche Urkunde im Sinne von § 415 ZPO zugrunde liegen und die kann nur von einer Behörde (Ämter oder Gerichte) oder einer mit öffentlichen Aufgaben betrauten Person stammen (zum Beispiel von einem Notar).

Im praktischen Betrieb sieht das anders aus, zumal dann, wenn der Schurkenprovider ausdrücklich dafür wirbt, dass bei ihm urheberrechtlich geschützte Werke oder Kinderpornographie zum illegalen Vertrieb gut aufgehoben sind, dass er Webshops vor den Nachstellungen betrogener Kunden schützt oder als weitere Dienste sichere Vertriebswege und vor allem das Inkasso anbietet (Hehlerei und Geldwäsche, §§ 259, 261 StGB). Je nach den Besonderheiten im Einzelfall begünstigt er seine Kunden (§ 257 StGB), begeht er Strafvereitelung (§ 258 StGB) oder beteiligt sich an den Taten seiner Kunden (mindestens) als Gehilfe (§ 27 Abs. 1 StGB), indem er die technischen Grundlagen für deren Taten schafft. Gegen die strafrechtliche Haftung kann ihn auch § 10 TMG (Privileg für den Hostprovider) nicht schützen, wenn er für kriminelle Zwecke wirbt und technische Vorkehrungen trifft, die mit legalen Kundennutzungen nicht in Einklang zu bringen sind.

In Einzelfällen trifft auch den Schurkenprovider eine selbständige strafrechtliche Haftung, wenn er Speicherplatz für Kinderpornos (§ 184b StGB), Zugangsdaten (Drops, § 202c Abs. 1 Nr. 1 StGB) oder für Programme für Computerstraftaten zur Verfügung stellt (§§ 202c Abs. 1 Nr. 2, 263a Abs. 3 StGB). Schafft er geschlossene Umgebungen für Personen, die ihrerseits eine kriminelle Vereinigung bilden, kann er sie damit auch unterstützen (§ 129 Abs. 1 StGB).

Dieses Ergebnis ist ernüchternd. Eine der von ihren kriminellen Auswirkungen her schwerwiegendsten Formen der organisierten Internetkriminalität kennt keine originäre Strafbarkeit, sondern nur eine abgeleitete, die sich auf die kriminellen Handlungen der Kunden und Partner bezieht.

Das bedeutet nicht, dass eine Strafverfolgung ausgeschlossen ist, sondern nur, dass zunächst erhebliche Anstrengungen erfolgen müssen, um die Taten der Kunden aufzuklären oder jedenfalls so zu umgrenzen, dass die Tatsache des Vorliegens von Straftaten zweifellos ist.

Dennoch besteht eindeutig eine ernste Strafbarkeitslücke in Bezug auf die organisatorischen Vorkehrungen der Schurkenprovider.

2.9.4 illegale Händler

Die Betreiber betrügerischer ▸ Webshops bilden einen wesentlichen Teil der Kunden von Schurkenprovidern. Der Schwerpunkt ihrer Strafbarkeit liegt im gewerbsmäßigen Betrug (§ 263 Abs. 1, Abs. 3 Nr. 1 StGB), wenn sie massenhaft auf Vorkasse oder Nachnahme Leistungen versprechen, die sie nicht erfüllen können.

Dieselbe Strafbarkeit betrifft die ▸ Abofallensteller. Sie handeln in der Tradition der Adressbuchverlage (Offertenbetrug) und treten seit ein paar Jahren vor allem mit dem Angebot des besonders schnellen Downloads von kostenfreien Programmen (Open Source) in Erscheinung [385].

Aus dem illegalen Handel mit urheberrechtlich geschützter Musik hat sich die kriminelle Szene fast vollständig zurückgezogen [386]. Ihnen haben die Tauschbörsen (Filesharing, Peer-to-Peer) den Rang abgelaufen.

Einträglich ist jedoch noch immer das Geschäft mit geschützten Kinofilmen, wie noch im Juni der Zugriff auf die Betreiber von kino.to gezeigt hat [387]. Ihnen wird die Bildung einer kriminellen Vereinigung zur gewerbsmäßigen Begehung von Urheberrechtsverletzungen vorgeworfen und sie verdienten wohl vor allem an massiven und häufigen Werbeeinblendungen. Die veröffentlichten Benutzerzahlen schwankten zwischen täglich 250 und 400 Tausend.

Auch andere Handelsgüter sind bereits von der Strafverfolgung aufgenommen worden, zum Beispiel der Handel mit Betäubungsmitteln (§§ 29 Abs. 1 Nr. 1, 29a Abs. 1, Nr. 1, Nr. 2 BtMG) und deren Grundstoffe (§ 19 Abs. 1 Nr. 1 GÜG), verschreibungs- oder apothekenpflichtige Arzneimittel (§§ 95, 96 AMG) und besonders solchen, die zum Doping verwendet werden (§ 95 Abs. 1 Nr. 2a, 2b AMG).

[385] Auf der Suche nach einem bekannten kostenfreien Antivirusprogramm wies mir die Suchmaschine zunächst mindestens sechs solcher Anbieter aus. Zu empfehlen sind hingegen die Angebote bei ▸ Heise, ▸ Chip, ▸ Computer Bild oder anderen Nachrichtenportalen.

[386] Dieter **Kochheim**, Cybercrime und politisch motiviertes Hacking, 20.10.2010, S. 6

[387] **CF**, kino.ko, 12.06.2011

2.9.5 Boards

Der Betrieb einer geschlossenen Benutzergruppe als solches ist nicht strafbar.

Das sieht anders aus, wenn ein Board ausdrücklich zu dem Zweck eingerichtet wird, dass es dem Erfahrungs- und dem sonstigen Austausch kriminell erlangter Daten, illegaler Dienste und Geräte dient.

Einen Schwerpunkt bilden die geschlossenen Gruppen, die sich dem Austausch kinderpornographischer Schriften und Dateien widmen. Die Verbreitungsverbote wegen Pornographie im Allgemeinen (§ 184 StGB), gewalt- oder tierpornographischer Schriften (§ 184a StGB), Kinderpornographie (§ 184b StGB) und Jugendpornographie (§ 184c StGB) dienen dem Schutz der sexuellen Selbstbestimmung der Abgebildeten und nicht zur Durchsetzung von religiösen oder bürgerlichen Moralvorstellungen. Das gilt besonders für die Kinderpornographie und damit meine ich weniger das Posen vorpubertärer Mädchen, sondern die Abbilder von Vergewaltigungen von Kleinkindern. Das Recht zu einer besonderen Schärfe zieht dieser Bereich des Strafrechts auch aus der Tatsache, dass erst die Abnehmer den Markt für die Anbieter schaffen. Dem Angebot von Bildern geht jedoch der sexuelle Missbrauch voraus.

Der Betreiber eines Kinderporno-Boards muss sich dieser Verantwortung stellen. Allein dadurch, dass er das Board eingerichtet hat und betreibt, fördert er das Verbreiten, Vorrätig halten und Anbieten kinderpornographischer Dateien und ist als Mittäter strafbar [388]. Bilden die Mitglieder des Benutzerkreises für sich eine kriminelle Vereinigung, ohne dass sich der Boardbetreiber daran beteiligt, unterstützt er diese Vereinigung (§ 129 Abs. 1 StGB), wenn er die Einrichtung des geschlossenen Kreises unter einschlägigen Schlagworten oder Namen zulässt, selber vornimmt oder – auch nur unterschwellig – dafür wirbt.

Einen zweiten Schwerpunkt bilden die eindeutig kriminell ausgerichteten Hackerboards. Das gilt besonders für die, die sich schon von ihrem Namen her besonderen kriminellen Praktiken widmen und bei näherer Betrachtung genau das tun.

Über die ▸ Carding-Boards habe ich bereits im Zusammenhang mit den ▸ Webshops berichtet. Schon mit ihren Namen strahlen sie Werbung für den kriminellen Umgang mit gestohlenen Daten von Zahlungskarten und anderen Formen des Identitätsdiebstahls mit anschließendem Missbrauch fremder persönlicher Daten aus. Das wird nicht besser, wenn man sich in ihrem Inneren umschaut [389].

Schon die eingerichteten Themengruppen (Threats) sind eindeutig und betreffen das Phishing, Skimming, Botnetze, Carding als solches und die besten Möglichkeiten, sich die erstrebte Beute zu sichern. Die Einrichtung der Threats überwachen die Administratoren. In ihren Innern wird locker über Straftaten berichtet, gestohlene Daten und Dienste angeboten und von irgendwelchen inneren Bedenken ist keine Spur zu bemerken [390].

Die schon vergessen geglaubten internen Webshops [391] sind wieder da. Für gutes Geld (60 bis 200 €) können Interessenten ein Monopol für bestimmte Dienste oder Waren erwerben, für Skimminggeräte, Botware, aber auch Rauschgift – streng getrennt nach Warengruppen: Heroin, Ko-

---

[388] Das folgt vor allem aus der Rechtsprechung zur Mittäterschaft zum Betrug anderer durch das Zurverfügungstellen eines Firmenmantels: **BGH**, Beschluss vom 29.04.2008 - 4 StR 125/08.

[389] Statt vieler: Marc-Aurél **Ester**, Ralf **Benzmüller**, G Data Whitepaper 2009. Underground Economy, 19.08.2009.

[390] Rivalisierende Gruppen hacken immer 'mal wieder ein gegnerisches Board und stellen den dabei gewonnenen Datenbank-Dump frei zugänglich ins Internet. Mit soliden Kenntnissen über SQL-Datenbanken lassen sich die Dumps wieder lauffähig machen. Sie geben erhellende und ernüchternde Einblicke in die Moralvorstellungen (irgendwo bei Null, außer wenn es um die eigene Szene geht) und Gedankenwelten der Beteiligten, die hemmungslos über ihre Taten plaudern und ihre kriminellen Geschäfte abwickeln.

[391] Marc-Aurél **Ester**, Ralf **Benzmüller**, Whitepaper 04/2010. Underground Economy - Update 04/2010, G Data 22.04.2010

kain und die anderen Gifte – Paketstationen und alle anderen Applikationen, die hilfreich für die Cybercrime im Allgemeinen sind.

Die organisatorische Herrschaft über solche offen kriminellen Boards haben die Betreiber und Administratoren, wobei wahrscheinlich Personalunion herrscht, sowie die in verschiedenen Service-Level-Stufen angesiedelten Moderatoren, die sich um die Diskussionen in den Threats kümmern. Sie und die Webshop-Berechtigten werden verbunden durch finanzielle Interessen. Die Betreiber und Administratoren verdienen an den Aufnahme- und Teilnahmegebühren, soweit sie erhoben werden, an den Monopollizenzen und ganz besonders an den Treuhandgebühren. Der Treuhänder empfängt den Kaufpreis und kehrt ihn erst an den Verkäufer aus, sobald der Käufer, den Empfang der Ware oder Leistung meldet (wie beim Notar oder bei eBay), nicht aber ohne seine Gebühr einzustreichen. Allein schon das ist Geldwäsche (§ 261 StGB).

Die Moderatoren genießen das besondere Vertrauen der Administratoren und sind deshalb von der Treuhandverpflichtung befreit. Das fördert ihren Gewinn (ohne Abzug der Treuhandgebühren) und ermöglicht es ihnen, die normalen Teilnehmer abzuziehen (was nur vorübergehend funktioniert).

Die Inhaber interner Webshops dürfen ihre Waren und Dienste exklusiv vermarkten. Ohne die Erwartung, dass sich das lohnt, kaufen sie keine Monopollizenz in einem geschlossenen Benutzerkreis, der eben auch nur eine beschränkte Zahl von Kunden hat.

Unter diesen Vorzeichen bilden die Betreiber, Administratoren, Moderatoren und Webshopbetreiber eine kriminelle Vereinigung (§ 129 StGB), deren Hinterleute die Betreiber und deren Rädelsführer die Administratoren und womöglich auch die Moderatoren sind (§ 129 Abs. 4 StGB). Die Teilnehmer unterstützen (mindestens) diese kriminelle Vereinigung und setzen sich allein deshalb der Bestrafung aus.

2.9.6 Inkassodienste und Beutesicherung

Paketagenten machen sich wegen Hehlerei (§ 259 StGB) und Finanzagenten wegen Geldwäsche strafbar (§ 261 StGB).

Inkassodienste für Webshops, die die komplette Auftragsabwicklung einschließlich Rechnungslegung und Forderungseinzug abwickeln (und sich dafür gut bezahlen lassen) sind jedenfalls beim Betrug (§ 263 StGB) Mittäter oder Gehilfen des Auftraggebers, weil sie den letzten Schritt der Tatbestandserfüllung, die Erlangung eines Vermögensvorteils, selbständig ausführen. Ansonsten sind sie genauso wie die anderen Zwischenhändler, die sich am Transfer der Beute beteiligen, in aller Regel Geldwäscher (§ 261 StGB).

Alle übrigen Formen müssen anhand des Einzelfalls betrachtet werden und lassen keine generelle Aussage über die Strafbarkeit zu außer der, dass irgendetwas an den Unterstützungshandlungen immer strafbar ist.

2.9.7 Spionage

Das Bild des Gesetzgebers von der IuK-Kriminalität ist geprägt vom Hacking, also dem Eindringen in fremde Computer, das Ausspähen und Abfangen von Daten und schließlich vom Missbrauch der mit dem Eindringen gewonnenen Macht.

Die seit etwa drei Jahren vorhergesagte und tatsächlich eingetretene Mehrung von individualisierten Angriffen gegen persönliche und gewerbliche Geheimnisse lässt sich mit den vorhandenen strafrechtlichen Instrumenten am besten greifen. Die technischen Methoden sind feiner und gemeiner geworden, unauffällig und nachhaltig. Das ändert nichts an der Tatsache, dass sie strafrechtlich recht einfach als das Ausspähen und Abfangen von Daten (§§ 202a Abs. 1, 202b StGB), als Computersabotage (§ 303b StGB), als das Ausspähen von Geschäftsgeheimnissen (§ 17 UWG) oder als ▸ Landesverrat verfolgt werden können.

Soweit private Geheimnisse betroffen sind, dümpelt die Strafbarkeit eher in den Bereichen der einfachen, allenfalls mittleren Kriminalität (Computerbetrug, § 263a StGB). Die Rechtsprechung des BGH fordert hingegen, die Perspektive auf die Tatfolgen und -hintergründe zu richten. Dadurch eröffnet sich hinter leichtkriminellen Handlungen häufig eine Perspektive, die die Rechtsordnung nicht mehr so locker und als schwere Kriminalität ansieht.

Dafür gibt es eine Reihe von Beispielen: Seit der richtungsweisenden Entscheidung des Großen Senats für Strafsachen wird die Bande nicht auf die Zusammenarbeit der Täter am Tatort beschränkt [392], sondern das arbeitsteilige Vorgehen als besonders gefährlich angesehen. Dazu gehört das Auskundschaften der Tatorte genauso wie die effektive Beutesicherung und ihr Absatz. Als konsequente Folge daraus sieht der BGH auch Vorbereitungshandlungen wie die Beschaffung eines Firmenmantels für die Ausführungstaten der Mittäter [393] als Täter- und nicht nur als Gehilfenhandlung an und selbst spontan wirkende Tatentschlüsse können sich als von einem gemeinsamen Bandenwillen getragen erweisen [394].

Im Zusammenhang mit Nazipropaganda hat der BGH die Bildung einer kriminellen Vereinigung ohne besondere Anforderungen sinnbildlich durchgewunken [395] und die Verabredung zu einem Verbrechen auf die Internetkommunikation [396] und auf die örtliche Zuständigkeit angewendet [397]. Das Skimming beschäftigt den BGH seit einigen Jahren. Er erkennt es im Ergebnis als das gewerbsmäßige Fälschen von Zahlungskarten mit Garantiefunktion an, wobei die Ausführungstat (Cashing) auch ein Computerbetrug ist [398]. Die eigentlich nur im Vorbereitungsstadium zum Fälschungsdelikt handelnden Ausspäher sind grundsätzlich als Mittäter der Fälscher anzusehen [399] und in arbeitsteiligen Strukturen können sie sich bereits am Versuch des Fälschens beteiligen, sobald sie die ausgespähten Daten an die Fälscher übermitteln [400].

Vor allem die jüngste Entscheidung über den Beginn des Versuchs beim Fälschen kennzeichnet den vorläufigen Schlussstrich hinter mehreren Entscheidungen, mit denen der BGH zunächst den Versuch beim optischen Fälschen von Zahlungskarten bestimmt [401], das Ergebnis auf das Skimming übertragen [402] und erst jüngst klargestellt hat: Das Skimming im engeren Sinne ist im Vorbereitungsstadium des Fälschens angesiedelt [403].

Diese Beispiele zeigen, dass die IuK-Kriminalität zwar ihre tatsächlichen Besonderheiten und speziellen Strafnormen hat, sie sich aber nicht hinter

---

392 **Großer Senat des BGH**, Beschluss vom 22.03.2001 - GSSt 1/00

393 **BGH**, Beschluss vom 29.04.2008 - 4 StR 125/08

394 **BGH**, Urteil vom 21.12.2007 - 2 StR 372/07

395 **BGH**, Beschluss vom 19.04.2011 - 3 StR 230/10

396 **BGH**, Beschluss vom 16.03.2011 - 5 StR 581/10

397 **BGH**, Beschluss vom 14.04.2011 - 1 StR 458/10

398 **BGH**, Beschluss vom 11.08.2011 - 2 StR 91/11

399 **BGH**, Urteil vom 17.02.2011 - 3 StR 419/10

400 **BGH**, Urteil vom 27.01.2011 - 4 StR 338/10

401 **BGH**, Urteil vom 13.01.2010 – 2 StR 439/09

402 **BGH**, Beschluss vom 14.09.2010 - 5 StR 336/10

403 **BGH**, Beschluss vom 11.08.2011 - 2 StR 91/11

einfach anmutenden, eher unbekannten und gnädig erscheinenden Strafvorschriften verstecken kann. Die Rechtsprechung zum Skimming zeigt, dass ganz schnell auch Verbrechen aus dem IuK-Strafrecht im weiteren Sinne Bedeutung erlangen, die keine Nachsicht zulassen und die auch wegen der Ermittlungsmaßnahmen eine nachdrückliche Strafverfolgung eröffnen. Kein anderer phänomenologischer Kriminalitätsbereich hat bereits im engeren Sinne eine solche Spannbreite von Bagatelldelikten (§ 202c StGB) bis zu schweren Verbrechen (gewerbsmäßiger Bandencomputerbetrug, § 263a Abs. 2 in Verbindung mit § 263 Abs. 5 StGB) wie das IuK-Strafrecht.

2.9.8 Söldner und Hacktivisten

Erst in jüngerer Zeit geraten auch die gewerblichen Experten in den Blick der Öffentlichkeit, die mit den Methoden des Hackings und des Social Engineering ebenso versiert umgehen wie Hacker und Kriminelle. Sie bieten ihre Dienste anderen Unternehmen, dem Militär, Geheimdiensten und anderen Interessenten an, um technische und organisatorische Sicherheitslücken in ihren Strukturen zu erkennen, Datenströme zu detektieren und Gegner zu identifizieren und zu bekämpfen [404]. Unternehmen wie HB Gary Federal und Partner, die trickreiche Strategien und Methoden zur Identifikation, Verfolgung und Blockade von Hacktivisten anbieten, oder das französische Unternehmen Vupen, das detektierte Sicherheitsmängel nur gegen Bezahlung benennt und behebt, bewegen sich in Tiefgraubereichen, die sich auch als strafbar erweisen können [405].

Das politisch korrekte Ziel, die atomaren Anreicherungsanlagen im Iran zu sabotieren, darf nicht darüber hinwegtäuschen, dass ▸ Stuxnet eine hochgefährliche Malware mit großem Missbrauchspotenzial ist. Sie kennzeichnet eine neue Dimension der Zerstörung, indem sie automatisch industrielle Steuerungsanlagen angreifen kann und zum Vorbild einer neuen Klasse von potentiellen Angriffen wird, die kriminell, militärisch und im Wettbewerb eingesetzt werden können.

Die Söldner agieren in Graubereichen, die wenig Aufsicht und Kontrolle kennen und dennoch nicht frei von rechtlichen Anforderungen sind. Datenauswertungen und -detektionen in Unternehmen mögen der Sicherheit nach außen und innen dienen, sie lassen sich aber auch zur Überwachung der eigenen Mitarbeiter missbrauchen, unterliegen den Datenschutz- und Mitbestimmungsregeln und sind nachhaltig dazu geeignet, das innere Unternehmensklima zu vergiften, wenn sie geheim durchgeführt und als subtiles Druckmittel eingesetzt werden.

Auch die Maßnahmen zur IT- und Unternehmens-

[404] Dieter **Kochheim**, Eskalationen, 20.02.2011, S. 15

[405] Dieter **Kochheim**, Eskalationen, 20.02.2011, S. 14

sicherheit müssen sich dem IuK-Strafrecht stellen und sind nicht bereits deshalb rechtmäßig, weil sie im unternehmerischen Auftrag erfolgen.

Auch die Hacktivisten von Anonymous [406] und LulzSec [407] oder Whistleblowing-Portale wie Wikileaks sind neue Qualitäten und bilden ungewohnte Herausforderungen. Sie erheben politische und moralische Ansprüche, was ebenfalls nicht darüber hinwegtäuschen darf, dass vor allem die Hacktivisten auch Straftaten begehen, wenn sie in die IT-Syteme von Gegnern eindringen, deren Webseiten verschandeln (Defacement) oder – wie Anonymous im Zusammenhang mit der Auseinandersetzung mit Wikileaks – DDoS-Angriffe gegen Wikileaks-Gegner und vor allem gegen die Banken führen, die Konten für Assange und Wikileaks blockierten, oder gegen Amazon, das Hostspeicher für Wikileaks gesperrt hatte.

Ein radikaler Teil der Internetgemeinde fordert die Einhaltung von Spielregeln ein! Unternehmen wie Amazon und große Finanzdienstleister können sich nicht mehr wie gewohnt selbstgerecht zurücklehnen, sich auf mehr oder weniger berechtigte AGB-Verstöße berufen, die ihnen so lange nicht aufgefallen sind, wie sie noch in Ruhe Geld verdienen konnten, oder gefahrlos politischem Druck aus dem Mainstream nachgeben. Die Angriffe von Anonymous machen sie zum Angriffsobjekt alternativen Wohlverhaltens. Das ist schmerzhaft! [408]

2.9.9 Abschaffung des Internet ?

Das Internet ist keine Enklave mehr, die unbeachtlich wäre oder für sich Sonderrechte oder Rechtsfreiheit beanspruchen kann. Die virtuelle und die reale Welt bestehen nebeneinander und verfügen fast überall über Berührungspunkte, durch die sie sich gegenseitig beeinflussen.

Die Finanzwirtschaft und der Warenhandel können sich aus der Netzwelt nicht mehr zurückziehen. Ohne Geldautomaten in aller Welt oder ohne Handelsplattformen müssten alle Arbeitsplätze wieder eingerichtet werden, die erfolgreich eingespart wurden. Und ohne sie würde eine ganze Menge (meiner) Lebensqualität verschwinden.

Die gegenseitige Durchdringung ist ein fortschreitender Prozess. Als vor 50 Jahren die universitären Großrechner, ihre Verbünde und die Hacker entstanden, waren sie zwar nicht ohne gesellschaftliche Bedeutung, nicht aber allgegenwärtig und überall und ständig präsent.

Politik, Wirtschaft und Gesellschaft haben zunächst nur vereinzelt, nicht aber programmatisch vorhergesehen, dass mit der IuK-Technik ein dunkles Zeitalter entstehen wird, weil die digitalisierten Daten der Zeitgeschichte Dank schnell marodierender Speichermedien verloren gegangen sind, schlecht normierte Formate heute nicht mehr verarbeitet werden können und die archivgerechte Dauersicherung von Kulturleistungen lange nicht versucht und noch weniger realisiert wurde.

Sie haben auch den Umgang mit den Umgebungsbedingungen einer digitalisierten Welt verschlafen, weil sie nicht vorhergesehen haben, was das Onlinebanking, die verzögerungsfreie weltweite (und gleichzeitig verschlüsselte) Kommunikation auch bedeuten: Kontroll- und Revisionsverlust (Nachvollziehbarkeit). Das gilt aber nicht nur für die restriktive Revision (Staatsaufgaben, Strafverfolgung), sondern auch für die gesellschaftliche (Politik, Informationsfreiheit als Grundlage für die Meinungsbildung und -freiheit).

Das ist ihnen aber nur bedingt vorzuwerfen. Der Vorwurf beschränkt sich darauf, dass die Methoden der Risikoerkennung und -bewertung unter-

---

406 **CF**, Anonymous vs. HBGary, 26.02.2011

407 **CF**, Sponti-Hacking: LulzSec, 13.06.2011

408 Dieter **Kochheim**, Eskalationen, 20.02.2011, S. 17

entwickelt waren und sind, so dass das Wachstum und die Folgen der IuK-Technik nicht vorhergesehen und strategisch begleitet wurden. Auch diese Aussage bedarf der Einschränkung: Auf welche Parameter hätten sich Risikobewertungen verlassen sollen, wenn sich die Entwicklungen völlig von klassischen Erfahrungen und Erscheinungen lösen und quasi zum Selbstläufer werden?

Eine rein konservative Reaktion wäre entwicklungsfeindlich und falsch.

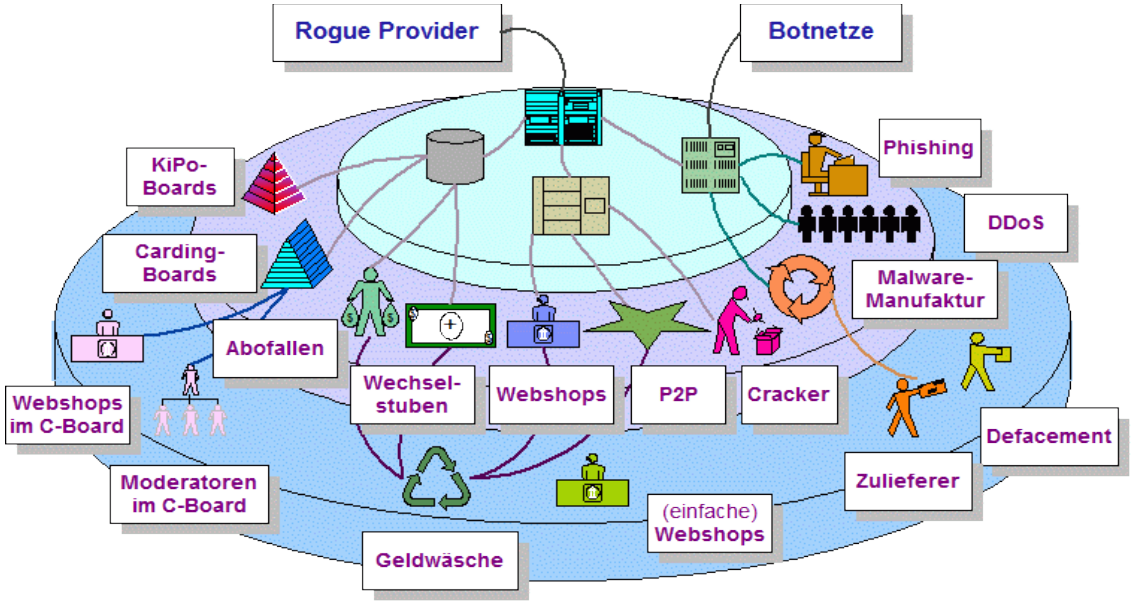
Wir müssen deshalb akzeptieren, dass es ein Nebeneinander zwischen realen und virtuellen Prozessen gibt und dass sie sich ständig gegenseitig beeinflussen und durchdringen. Wir müssen akzeptieren, dass sich dieser Prozess nicht umkehren lässt, wenn wir nicht gleichzeitig alle Vorteile der virtuellen Dienste verlieren wollen (und uns fellbekleidet und keulendrohend zu sachlichen Tauschgeschäften zusammenfinden wollen).

Deshalb müssen wir auch akzeptieren, dass die Cyberkriminellen alle Schlupflöcher nutzen, die sich ihnen bieten, dass neue Geschäftsfelder für Söldner entstehen und dass auch die Zivilgesellschaft (Hacktivismus) sich gegen die anderen Erscheinungsformen aufstellt.

Darauf müssen sich auch Politik und Strafverfolgung einstellen. Es reicht nicht aus, dass besondere Spezialabteilungen bei der Polizei oder den Staatsanwaltschaften aufgebaut werden, deren – vor allem personelle – Ausstattung Lücken an anderen Stellen reißen. Vielmehr bedarf es neben einer besonderen Ausbildung für Spezialisten auch einer breiten Ausbildung für alle Beteiligten. Erst sie schafft Sensibilität für die IuK-Kriminalität, macht sie sichtbar, bewertbar und verfolgbar. Daneben bedarf es einer strategischen Bewertung der IuK-Kriminalität, um ihre Bedeutung, Verbreitung und Verfolgung messbar zu machen, Schwerpunkte zu setzen und das Vorgehen zu planen.

2.10 Strukturelle Betrachtung der Cybercrime

Ein Bild sagt wahrscheinlich mehr aus als viele Worte:



Der Blick auf die Strukturen der Cybercrime zeigt ein vielgestaltiges Bild von den weitgehend einzeln oder in kleinen Gruppen handelnden Akteuren. Die Grafik betrachtet drei verschiedene Arbeitsebenen. Auf der inneren Scheibe (hellblau) handeln die Cyberkriminellen, die eine eigene technische Infrastruktur aufbauen, betreiben und erhalten. Auf dieser Ebene des ***technischen Betriebes*** handeln vor allem die ▸ Schurkenprovider nach dem Vorbild des Russian Business Network – RBN – und die Betreiber der ▸ globalen Botnetze.

Die Basis für meisten kriminellen Aktivitäten stellen die Rogue Provider zur Verfügung. Nur Dank ihrer technischen Tricks und festen Einbindung in die sonstigen Strukturen des Internets können sie allen anderen erst den „sicheren Hafen“ für ihre betrügerischen Webshops oder anderen Handlungen zum Beuterwerb und ihrer Sicherung liefern. Dagegen liefern die Botnetzbetreiber nur die Werkzeuge, um DDoS-Angriffe oder Datendiebstähle durchzuführen.

Die Akteure auf der mittleren Scheibe richten einen ***administrativen Betrieb*** ein und nutzen dazu die technische Infrastruktur, die einen Missbrauch ermöglichen oder die ihnen von den technischen Betreibern zur Verfügung gestellt werden.

Auf dieser Ebene sind die ***Betreiber*** von Webshops, Abofallen, Boards verschiedener Ausprägungen und anderer kriminellen Erscheinungsformen tätig, auf die im Zusammenhang mit der ▸ Organisierten Internetkriminalität eingegangen wird. Es handelt sich dabei um professionelle Kriminelle. Hier siedele ich auch die Malware-Manufakturen, die modernen Phisher und die Betreiber von Filesharing- und Streaming-Diensten an, wenn sie sich dem profitablen Vertrieb von Vorpremierenfilmen oder (unlizensierter) kommerzieller Software widmen.

Auf der untersten Scheibe agieren die aktiven Mitläufer, die durchaus gewerbsmäßig handeln, aber dazu keine eigene technische oder administrative Infrastruktur schaffen. Dazu gehören zum Beispiel die Moderatoren und Webshop-Betreiber innerhalb von geschlossenen Carding-Boards, aber auch Organisatoren von Operation Groups, die Finanz- und Paketagenten führen oder mit Bankkonten unter falschen oder vorgeschobenen Identitäten handeln.

Die hier gewählte Betrachtungsweise ist eine technische. Sie kann nur begrenzt die kriminelle Gefährlichkeit der Handlungen abbilden. Dennoch zeigt sie recht gut die Abhängigkeiten der kriminellen Szene: Ohne Schurkenprovider ginge fast nichts.

In Bezug auf die administrative und die Mitläufer-Ebenen ist das Modell sehr grob und sagt nicht viel über die aufgewendete kriminelle Energie aus. Auch personale Strukturen oder gar Banden lassen sich mit ihm nicht abbilden. Es gibt aber einen Eindruck von den kriminellen Vorbereitungshandlungen, die zum Anschub nötig sind.

3. Stand und Zustand des IuK-Strafrechts

Die Auseinandersetzungen mit dem IuK-Strafrecht zeigen, dass es auch bei modernen Formen der Kriminalität nicht versagt, aber Lücken und systematische Schwächen aufweist, die das Verständnis und seine Anwendung erschweren.

Anlass zum Alarm und zur unverzüglichen Revision des IuK-Strafrechts gibt es nicht, weil viele Strafbarkeitslücken bei genauer Betrachtung keine sind. Dennoch zeigt das gesetzliche System strukturelle Probleme, Lücken und Schwächen auf, die mittelfristig nach einer Revision verlangen.

Diese Schwächen im geltenden Recht sollen hier beschrieben werden, um Risiken zu benennen und die Diskussionen zu fördern. Handlungsbedarf sehe ich vor allem bei der Bereinigung des Strafrechts der Vorbereitungshandlungen, wegen der fehlenden Datenhehlerei und der ausstehenden Auseinandersetzung des Gesetzgebers mit den modernen Ausprägungen der Cybercrime, vor allem mit der Malware, der Botware, den kriminellen Boards und den Schurkenprovidern.

Die weitere Diskussion kann zum Ergebnis haben, dass Gesetzesänderungen nicht erforderlich sind. Auch das ist ein Ergebnis, das dem Fachpublikum und einem demokratischen Rechtsstaat angemessen ist. Es würde zeigen, dass jedenfalls die Risiken benannt, bewertet und wegen ihrer Folgen abgeschätzt wurden. Nichts ist gefährlicher als blind in Entwicklungen und Fallen zu laufen.

3.1 systematische Schwächen

Das IuK-Strafrecht hat keine eigene Systematik, sondern im Wesentlichen vier besondere Ansatzpunkte, an denen es in die Systematik des StGB eingefügt wurde:

- Strafrechtlicher Datenschutz bei der Verletzung des persönlichen Lebens- und Geheimbereichs: §§ 202a Abs. 1, 202b, 202c StGB.
- Körperlicher Schutz gegen Sachbeschädigung: §§ 303a, 303b StGB.
- Computerbetrug: § 263a StGB.
- Schutz des Rechtsverkehrs bei der Datenverarbeitung: §§ 268, 269, 270, 271, 274 Abs. 1 Nr. 2 StGB.

Dieses gesetzestechnische Vorgehen hat den Vorteil, dass die Besonderheiten der Datenverarbeitung dem Rechtsgüterschutz der übrigen Tatbestände zugeordnet werden und ihn ergänzen. Im Umgekehrten sind die Vorschriften des IuK-Strafrechts nicht nur aus ihrem Zusammenhang als besondere Vorschriftengruppe heraus auszulegen, sondern vor allem anhand der Rechtsgüter und der Systematik der Abschnitte im StGB, in die sie eingefügt wurden. Das macht die Betrachtung der IuK-Straftaten mit ihren Gemeinsamkeiten und Zusammenhängen unübersichtlich und schwierig.

Die Auslegung der IuK-Strafnormen verlangt nach mehreren Prüfungsstufen, um ihre Regelungsgrenzen zu erkunden:

- Die natürliche Grenze der Auslegung ist der Wortlaut der Norm. Für das materielle Strafrecht gilt zu Recht ein Analogieverbot (§ 1 StGB, Art 103 Abs. 2 GG).
- Eine systematische Verbindung zwischen verschiedenen Normen des IuK-Strafrechts bilden zum Beispiel die Datendefinition in § 202a Abs. 2 StGB und die ausdrückliche Benennung von Passwörter oder sonstige Sicherungscodes in § 202c Abs. 1 Nr. 1 StGB, worauf verschiedene andere Vorschriften verweisen.
- Die Systematik des Abschnitts, in die sie eingesetzt ist, prägt die IuK-Strafnorm. Das wird beson-

ders deutlich am Abschnitt über die Urkundenfälschungen: Die schriftliche Lüge und die Verwendung eines offensichtlichen Abbildes vom Original sind unter dem Gesichtspunkt der Urkundenfälschung straflos.

▸ Nach der Erfassung des Wortsinns und des systematischen Zusammenhangs einer IuK-Strafnorm greift bei verbleibenden Zweifeln die verfassungskonforme Auslegung. Für sie ist, das haben meine Überlegungen gezeigt, besonders wichtig das Urteil des BVerfG zur Onlinedurchsuchung [409], womit das BVerfG das neue Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme entwickelt [410] und das den strafrechtlichen Schutz dieser allgegenwärtigen Systeme verdeutlicht und verstärkt hat.

Die Unübersichtlichkeit des IuK-Strafrechts zeigt sich noch mehr bei den strafbaren Vorbereitungshandlungen und in erster Linie in den überraschenden Rückverweisen auf § 202c StGB in den §§ 303a Abs. 3, 303b Abs. 5 StGB, die sich einem ersten Blick in das Gesetz verschließen. Ein Laie hat kaum eine Chance, diese Zusammenhänge zu erkennen, wenn er nur das Gesetz liest (siehe unten wegen der Einzelheiten).

Hinzu kommen strukturelle Mängel im Detail:

Das bestehende IuK-Strafrecht im engeren Sinne genügt schon nicht dem Anspruch des Gesetzgebers, der Abhörschutz sei vollständig gewährt. Neben dem Ausspähen (sozusagen beim „Hacking“, § 202a Abs. 1 StGB) und dem Abfangen (sozusagen beim „Abhören“, § 202b StGB) ist vom funkrechtlichen Abhörverbot (§ 148 Abs. 1 Nr. 1. TKG) der Amateurfunk ausgenommen (§ 89 TKG). Die ihm zugewiesenen „Amateurbänder“ [411] sind teilweise deckungsgleich mit den Frequenzbändern, in denen der Nahfunk bei der Bluetooth-Technik und in denen die mittleren Frequenzbänder für lokale Funknetze (WLAN [412]) liegen.

Die Datendefinition in § 202a Abs. 2 StGB beschränkt sich auf den Schutz gespeicherter oder übermittelter („fließender“) Daten. Der Vorgang der manuellen Dateneingabe wird davon nicht erfasst. Das hat jedenfalls Auswirkungen auf die Rechtsfragen beim Skimming, weil das Ausspähen der Tastatureingaben für die PIN mit Kameras datenstrafrechtlich nicht erfasst wird. Dasselbe gilt beim Einsatz von Tastaturauflagen. Bei ihnen erfolgt der Datenabgriff mechanisch und ist dem Datenverarbeitungsprozess im Geldautomaten räumlich vorgeschaltet. Die oberen Tasten wandeln den Tastendruck zwar in elektromagnetische Signale um, aber erst der Stift am unteren Ende der oberen Taste gibt den Tastendruck an die originale Taste vom Geldautomaten weiter [413].

Ob der vom Gesetzgeber gewählte Weg, kein selbständiges IuK-Strafrecht zu schaffen, weise war, lässt sich noch nicht abschließend beurteilen. Wie sich zeigen wird, weist es auch noch andere Schwächen auf, die eine Revision des IuK-Strafrechts dringend fordern.

---

[409] **BVerfG**, Urteil vom 27.02.2008 - 1 BvR 370/07, 595/07, Rn 166

[410] Einzelheiten: Dieter **Kochheim**, Verdeckte Ermittlungen im Internet, 27.07.2011, S. 15 (Integrität informationstechnischer Systeme).

[411] Amateurband

[412] **CF**, Abgrenzungen, 2007

[413] Beim POS-Skimming ist es eine dünne Folie, die zwischen die Tastatur und der Elektronik im Terminal eingesetzt wird.

3.2 strafbare Vorbereitungshandlungen

Vorbereitungshandlungen wie die Beschaffung von Tatwerkzeugen oder das Auskundschaften von Tatorten sind grundsätzlich straffrei. In Bezug auf Vergehen (§ 12 Abs. 2 StGB) gilt das auch für den Versuch, wenn seine Strafbarkeit nicht ausdrücklich vom Gesetz vorgesehen ist (§ 23 Abs. 1 StGB). Etwas anderes gilt jedoch für Verbrechen, also für Straftaten, die mit mindestens einem Jahr Freiheitsstrafe bedroht sind (§ 12 Abs. 1 StGB). Ihr Versuch ist immer strafbar (§ 23 Abs. 1 StGB) und bereits die Anstiftung zu einem Verbrechen sowie seine Verabredung sind schon eine vorgelagerte Beteiligung und deshalb strafbar (§ 30 StGB).

In einer Reihe von Fällen und das verstärkt im Hinblick auf IuK-Straftaten hat der Gesetzgeber eine besondere Strafbarkeit im Vorbereitungsstadium geschaffen (siehe Bild auf der Folgeseite), die sich vor allem an dem „Hackerparagraphen“ orientiert (§ 202c StGB). Er beschränkt sich auf Passwörter und Sicherungscodes, also im wesentlichen auf die Zugangsdaten zu individuellen Konten, Zugangs- und Ausführungsrechten, sowie auf Computerprogramme, deren besonderer Zweck das Abgreifen oder die Veränderung von Daten ist.

Die Gefährdungstatbestände des IuK-Strafrechts beschränken sich wegen der Werkzeuge auf die Computerprogramme und kennen kein Hardwareverbot. Eine gesetzliche Definition für „Computerprogramme“ fehlt, so dass vor allem Zweifel an der geforderten Funktionstiefe [414] bestehen. Eine gewisse Klarheit hat das BVerfG nur im Hinblick auf die Zweckbestimmung geschaffen [415]: *Tatobjekt des § 202c Abs. 1 Nr. 2 StGB kann nur ein Programm sein, dessen Zweck die Begehung einer Straftat nach § 202a StGB ... oder § 202b StGB ... ist. Danach muss das Programm mit der Absicht entwickelt oder modifiziert worden sein, es zur Begehung der genannten Straftaten einzusetzen.*

Besonders deutlich werden die aufgezeigten Probleme beim Skimming im engeren Sinne, also beim Abgreifen der Kartendaten und der PIN. Über die §§ 152a Abs. 5, 152b Abs. 5 StGB gilt hier auch § 149 Abs. 1 Nr. 1 StGB, der den Umgang mit *Computerprogrammen oder ähnliche Vorrichtungen* unter Strafe stellt, *die ihrer Art nach zur Begehung der Tat geeignet sind*. Nach früherem Gesetzeswortlaut waren keine Kartenlesegeräte (Skimmer) erfasst [416]. Das sieht der BGH nach geltendem Recht anders [417].

Die PIN-Skimmer (Kameras, Tastaturaufsätze) dienen jedoch nicht dem ***Fälschen*** von Zahlungskarten, sondern erst zur Sicherung des ***Gebrauchs*** der Fälschungen mit dem damit einhergehenden Computerbetrug [418], so dass sie von § 149 StGB nicht erfasst sind. Einschlägig für die Vorbereitungstat ist deshalb § 263a Abs. 3 StGB, wonach nur der Umgang mit Computerprogrammen und nicht auch mit „ähnlichen Vorrichtungen“ strafbewehrt ist. PIN-Skimmer unterliegen deshalb einer Strafbarkeit als Beziehungsgegenstand nur, wenn ihre elektronische Schaltung auf das Ausspähen ausgerichtet wurde, und nicht bereits, wenn an ein handelsübliches Handy ein weiterer Akku angelötet wurde.

§ 202c StGB droht im Höchstmaß mit einer Freiheitsstrafe von einem Jahr und ist damit im Bereich der einfachen Kriminalität angesiedelt [419].

---

[414] Gemeint ist eine Entsprechung zur Originalität, die im Zusammenhang mit den Urheberrechten diskutiert wird (Werktiefe).

[415] Dual Use: **BVerfG**, Beschluss vom 18.05.2009 - 2 BvR 2233/07, Rn 60.

[416] Inzwischen überholt: **BGH**, Urteil vom 16.12.2003 - 1 StR 297/03.

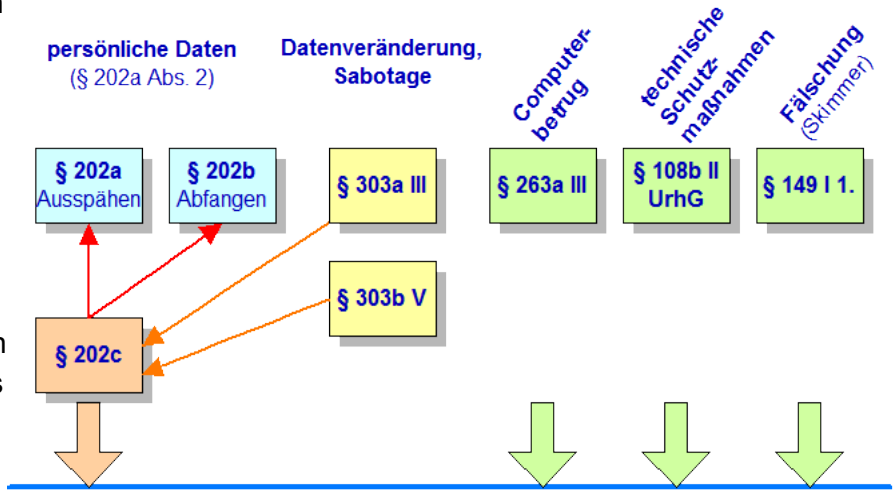
[417] Der BGH lässt die tatbestandliche Frage und die nach der Konkurrenz zur Verbrechensabrede ausdrücklich offen (BGH, Urteil vom 17.02.2011 – 3 StR 419/10, Rn 12), hat aber schon mehrere Verurteilungen nach § 149 StGB kommentarlos „durchgewunken“ (BGH, Beschluss vom 12.05.2011 - 3 StR 101/11). Nach Ansicht des 2. Strafsenats verdrängt die Verbrechensabrede den § 149 StGB (BGH, Urteil vom 13.01.2010 - 2 StR 439/09, Rn 16).

[418] Zuletzt: **BGH**, Beschluss vom 11.08.2011 - 2 StR 91/11, Rn 13.

[419] Die gesellschaftlichen Wirkungen der Verfolgung einfacher Kriminalität sind nicht unbeachtlich. Das beweist die Trunkenheit im Verkehr (§ 316 StGB), die auch nur mit einem Jahr Freiheitsstrafe droht.

§ 263a Abs. 3 StGB droht hingegen mit drei Jahren Freiheitsstrafe und § 149 StGB sogar mit fünf Jahren. Darin kommt ein Wertungswiderspruch zwischen diesen Vorbereitungshandlungen zum Ausdruck, der in dieser Ausprägung kaum nachvollziehbar ist.

Wünschenswert wäre eine Revision und Zusammenfassung wenigstens des Strafrechts der Vorbereitungshandlungen wegen IuK-Straftaten. Sie könnte die Strafbarkeit auf die Hardware erweitern, die strafrechtlichen Anforderungen an die Funktionstiefe von Computerprogrammen präzisieren und entschärfen und schließlich ein geschlossenes und stimmiges System der strafbaren Gefährdungsdelikte schaffen.



3.3 materielle Lücken

Die Datenhehlerei als solche ist nicht strafbar. Sie könnte nach dem Vorbild der Hehlerei (§ 259 StGB) den Handel mit gestohlenen persönlichen, gewerblichen und nicht öffentlichen Daten einschließlich der Absatzhilfe umfassen und auf gewerbs- und bandenmäßige Formen der Kriminalität reagieren. Teilbereiche der Datenhehlerei werden jetzt von § 202c Abs. 1 Nr. 1 StGB wegen der Zugangsdaten, von § 17 Abs. 2 Nr. 1 lit a und b UWG wegen der Betriebs- und Geschäftsgeheimnisse und § 44 Abs. 1 BDSG wegen personenbezogener Daten abgedeckt, *die nicht allgemein zugänglich sind* (§ 43 Abs. 2 BDSG).

Dieses von drei verschiedenen Normen geprägte System mag wichtige Teile der Verwertung geklauter Daten abdecken. Die drei Strafvorschriften bilden jedoch keine einheitliche Linie und werden im Anwendungsfall durch fachrechtliche Einschränkungen und andere Vorbehalte beschränkt (Strafantrag, § 44 Abs. 2 BDSG):

- § 202c Abs. 1 StGB ist im Bereich der einfachen Kriminalität angesiedelt und ermächtigt deshalb nur zu üblichen Ermittlungen (Auskünfte, Durchsuchung, einmalige E-Mail-Beschlagnahme).
- § 17 Abs. 2 UWG verlangt nach einem wettbewerblichen Bezug. Wenn der nicht hergestellt werden kann, bliebe allenfalls das technische Aufzeichnungsverbot nach § 201 StGB, das nur einen kleinen Teil der Daten umfasst, die mit technischen Mitteln oder mit dem Social Engineering er-

kundet werden können. Die Grundtatbestände beider Vorschriften sind ebenfalls im Bereich der einfachen Kriminalität angesiedelt.

▸ Die Strafverfolgung wegen eines besonderen Datenschutzdelikts erfordert einen Strafantrag des Datenschutzbeauftragten (§ 44 Abs. 2 BDSG). In diesen Fällen ist die Staatsanwaltschaft zwar zu vorläufigen Ermittlungsmaßnahmen berechtigt (Nr. 6 RiStBV), die jedoch – auch in Anbetracht der Strafdrohung von höchstens zwei Jahren Freiheitsstrafe – recht oberflächlich bleiben müssen.

Weitere Lücken betreffen die Verlässlichkeit von Aussagen über die eigene Identität im Datenverkehr und den Aussagewert von Abbildungen und anderen Belegen. Dabei geht es mir nicht um die Frage der Anonymität, sondern um „schriftliche Lügen“ und Fälschungen ohne das Erfordernis, dass sie zur Täuschung im Rechtsverkehr erfolgen.

Der Schutz des Rechtsverkehrs im Zusammenhang mit Urkunden (§ 267 StGB) ist auf das Original beschränkt, was bereits aus dem klaren Wortlaut des § 267 Abs. 1 StGB spricht. Davon ist der Schutz in Bezug auf Kopien, Faxe und Abbildungen in Dateien ausgenommen, was im Rahmen der bestehenden Vorschriften verständlich ist.

Dem folgend greift die Strafbarkeit der Fälschung beweiserheblicher Daten (§ 269 StGB) in aller Regel erst dann, wenn sie besonders gesichert sind, zum Beispiel durch eine qualifizierte Signatur (§ 2 Nr. 3 SigG). Die Interessen des Geschäfts- und Rechtsverkehrs lassen dennoch einen Abbildschutz als wünschenswert erscheinen, der unterhalb des Urkundenschutzes im Bereich der einfachen Kriminalität angesiedelt wäre. Über seinen Sinn und seine Gestalt im Einzelnen muss an anderer Stelle diskutiert werden.

Für das IuK-Strafrecht wäre ein niederschwelliger Abbild- und Lügenschutz vor allem im Hinblick auf erlogene Absenderangaben und Links bei Spam-Mails und bei der Maskierung von Servermeldungen sowie bei der Whois Protection wünschenswert. Auch darüber müsste bei der fälligen Revision des IuK-Strafrechts wenigstens nachgedacht werden.

Das geltende IuK-Strafrecht orientiert sich am Hacking und dem Eindringen in fremde Datenverarbeitungsanlagen. Die Fernsteuerung von Zombies in einem Botnetz, der Identitätsdiebstahl durch Missbrauch fremder informationstechnischer Systeme und die Funktionen autonomer Malware sind ihm fremd. Das führt dazu, dass im Anwendungsfall die Strafbarkeit aus fernliegend erscheinenden Vorschriften oder solchen der Organisationsstrafbarkeit abgeleitet werden müssen. Die erörterten Beispiele belegen, dass kaum straflose Räume bestehen, wohl aber jede Menge praktische Schwierigkeiten.

Im Zusammenhang mit den strafbaren Vorbereitungshandlungen ist deshalb auch zu diskutieren, wie der Gesetzgeber mit präparierten Webseiten, Pharmen und der Verteilung von Malware beim Spamming umgehen will.

3.4 Organisierte IuK-Kriminalität

Meine Ausführungen zur Organisierten IuK-Kriminalität sind qualitativer Art und können keine Aussagen zu ihrer Verbreitung und ihrem tatsächlichen Gefährdungspotenzial leisten. Nur so viel: Es gibt sie und es gibt sie auch im Inland. Wenn sie von der Strafverfolgung unbehelligt bleiben, dann werden sich die Täter weiterhin als unantastbar sehen und ihre Aktivitäten werden sie nicht einstellen. Sie werden weitere geneigte Täter hinzugewinnen und die kriminelle Qualität wird weiter steigen. Aber auch das sind qualitative Aussagen ohne quantitative Untermauerung.

Das Organisationsstrafrecht im weiteren Sinne beruht auf der Mittäterschaft (§ 25 Abs. 2 StGB) und der weitsichtigen Rechtsprechung des BGH zur kriminellen Arbeitsteilung am Rande der Tatvollendung, dem Bandenstrafrecht und schließlich auf der kriminellen Vereinigung (§ 129 StGB), in der auch die Rädelsführer und Hinterleute der Strafverfolgung ausgesetzt sind. Es liefert (noch grobe) Instrumente, um arbeitsteilige Tätergruppen im Zusammenhang mit Boards, Botnetzen und Malware-Fabriken zu verfolgen. Die noch ausstehenden Erfahrungen werden zeigen, ob die Instrumente geeignet sind.

Ich vermute aber, dass auch spezielle Normen und Methoden entwickelt werden müssen, um gegen diese Erscheinungsformen vorzugehen. Das beruht vor allem darauf, dass die Anwendung allgemein formulierter Strafnormen auf besondere Sachverhalte sehr zähe Ermittlungen, Beweisaufnahmen und Auseinandersetzungen nach sich ziehen. Das lässt Um- und Irrwege in der Spruchpraxis der Gerichte erwarten, die erst im weiteren Verlauf zu einer geraden Linie werden. Im Zusammenhang mit dem Skimming hat es jedenfalls der BGH binnen drei Jahre geschafft, die wesentlichen Fragen zu lösen und sinnvolle Perspektiven aufzuzeigen. Das war schnell und doch zu langwierig, um mit den kriminellen Innovationen Schritt zu halten.

Der Gesetzgeber ist seit 2007 untätig geblieben. Es wäre wünschenswert, wenn er sich zum Spamming, zur autonomen Malware, zu den Boards und zu den Schurkenprovidern positioniert. Das wird noch ein paar weitere Jahre dauern.

3.5 Ermittlungen gegen die IuK-Kriminalität

Die schwersten Straftaten im IuK-Strafrecht sieht der Gesetzgeber in den Verbrechen des Cashing (Fälschen und Gebrauchen von Zahlungskarten mit Garantiefunktion, § 152b StGB) und in den beiden selbständigen Qualifikationen des gewerbsmäßigen Bandencomputerbetruges (§§ 263a Abs. 2, 263 Abs. 5 StGB) sowie der gewerbsmäßigen Bandenfälschung technischer Aufzeichnungen (§§ 268 Abs. 5, 267 Abs. 4 StGB) und beweiserheblicher Daten (§§ 269 Abs. 3, 267 Abs. 4 StGB). Ihnen folgen die besonders schweren Fälle des Computerbetruges (§§ 263a Abs. 2, 263 Abs. 3 StGB), der schweren Computersabotage (§ 303b Abs. 4 StGB), der Fälschung technischer Aufzeichnungen (§§ 268 Abs. 5, 267 Abs. 3 StGB) und beweiserheblicher Daten (§§ 269 Abs. 3, 267 Abs. 3 StGB). Mit ihren Strafdrohungen bis zu zehn Jahren Freiheitsstrafe kennzeichnen sie Fälle der schweren Kriminalität und mit Ausnahme des besonders schweren Falles der schweren Computersabotage sind sie alle in den Straftatenkatalog des § 100a Abs. 2 Nr. 1 n), p) StPO aufgenommen worden [420]. Wegen ihrer Strafverfolgung sind damit fast alle Ermittlungsmethoden zugänglich, die die StPO zur Verfügung stellt.

Aus dem IuK-Strafrecht im weiteren Sinne sind zum Beispiel auch der Umgang mit kinderpornographischen Schriften (§ 184b Abs. 1 bis 3 StGB), die Beteiligung an einer kriminellen Vereinigung (§ 129 StGB) und die Volksverhetzung (§ 130 StGB) im Straftatenkatalog des § 100a Abs. 2 StPO erfasst.

Die Ermittlungen im Bereich der IuK-Kriminalität machen es nötig, zunächst sehr genau die Art der Tatausführung und die materielle Bedeutung der Straftat zu durchdenken. Im Bereich der ▸ Onlinebanking-Trojaner gelangen wir dadurch schnell zum Vorwurf des gewerbsmäßigen Betruges und wegen ▸ verteilter Angriffe zur gewerbsmäßigen Computersabotage und zur besonders schweren Erpressung. Anders sieht es aus wegen der „klassischen“ Hacking-Taten, die sich häufig nur als Formen der einfachen Kriminalität im Zusammenhang mit dem Ausspähen von Daten und der Datenveränderung darstellen.

Die Beweismittel im Zusammenhang mit der IuK-Kriminalität stellen besondere Anforderungen an ihre Erhebung und Bewertung. Wegen der ▸ Göttinger Abofalle musste das Landeskriminalamt die von den Tätern genutzte Software minutiös analysieren, um ihnen nachzuweisen, dass sie automatisch die IP-Adressen der Besucher erhob und zu den bereits vorhandenen Personendaten speicherte, und nur daraus leiteten die Täter ihre vermeintlichen Forderungen ab. Auch die Funktionsweisen von Onlinebanking- und Botnetz-Malware müssen fachkundig betrachtet werden, um ihre Funktionsweise im einzelnen zu verstehen. Und schließlich: Ohne Verkehrs- und Vorratsdaten lassen sich die Spuren zu den versteckt handelnden Tätern niemals nachverfolgen.

Die Identifikation von Tätern und den Standorten ihrer Technik erfordert den Einsatz von Messinstrumenten, die überwiegend frei zugänglich sind, und ihren geschulten Einsatz durch Fachleute. Diese müssen in der Lage sein, die Ergebnisse ihrer Erkundungen deutlich und verständlich machen. Es gilt, alle Verfahrensbeteiligten vom Ergebnis zu überzeugen und keine Angriffspunkte zu liefern, die sie angreifbar oder wertlos machen. Die dazu entwickelten Standards haben sich noch nicht in aller Breite durchgesetzt und müssen ihre Praxistauglichkeit erst noch beweisen.

Ohne weitere Anhaltspunkte, Tests oder Protokolle ist der schlichte Aussagewert von Daten gering. Das gilt jedenfalls für Verkehrsdaten und Programme, weniger für sinnlich wahrnehmbare Texte, Abbildungen und Kompositionen wie Webseiten. Aber auch in ihren Trägermedien können sich Funktionen verstecken, die sich erst beim Blick auf den Quellcode oder auf verbundene Quellen erschließen.

Zu geschlossenen Benutzerkreise und sozialen Netzwerken bekommt die Strafverfolgung regel-

[420] Keines der Delikte rechtfertigt einen Großen Lauschangriff nach § 100c StPO. Siehe auch: **CF**, Straftatenkatalog, 2007.

mäßig nur Zugang dadurch, dass sie sich an ihnen beteiligt. Die dabei gewonnenen Erkenntnisse müssen unmissverständlich dokumentiert, nachvollziehbar und revisionssicher sein. Auch das ist keine leichte Aufgabe.

Die wenigen Beispiele zeigen, dass das IuK-Strafrecht nicht nur im materiellen Bereich besondere Anforderungen stellt, sondern auch im formellen, also im Verfahrensrecht. Sie zeigen auch punktuelle Erfolge, die dadurch möglich wurden, dass Strafverfolger und Richter ihre Aufgaben ernst genommen und sich in die Themen von Neuländern eingearbeitet haben. Ohne die Leistungen anderer zu schmälern: Den wichtigsten Anteil an der Verfolgung der IuK-Kriminalität hat die Polizei, die ihre Erscheinungsformen wahrnehmen und die gebotenen Ermittlungen professionell durchführen muss. Dazu wurden Fachleute ausgebildet und gefördert, die dann die Schwierigkeit haben, ihre Erkenntnisse und Schlüsse so zu vermitteln, dass sie verständlich und schlüssig sind.

Das ist kein einseitiger Prozess. Auch unerfahrene Kollegen sind in der Pflicht, sich den Anforderungen der IuK-Kriminalität zu stellen. Das heißt auch, sich mit den technischen Fragen und Funktionen so weit vertraut zu machen, dass man ihre Wirkungen und Zusammenhänge versteht. Von ihnen wird keine technische Ausbildung oder ein Informatik-Studium verlangt, wohl aber ein Grundverständnis, das in anderen Kriminalitätsbereichen längst selbstverständlich ist (zum Beispiel wegen Straßenverkehr und Kfz-Technik, Wirtschaft und Buchführung, Medizin und Psychiatrie).

Ungeachtet dessen sind auch die Verwaltungen und die Politik gefragt. Die Verfolgung der IuK-Kriminalität muss man wollen und man bekommt keine Erfolge zum Nulltarif, sondern nur, wenn man Fortbildung leistet und Freiräume schafft, damit sich die Betreffenden in die Themen einarbeiten können.

4. Schluss

Das vorliegende Arbeitspapier gibt einen Überblick über die Erscheinungsformen der IuK-Kriminalität und ihre strafrechtliche Bewertung. Es zeigt eine Reihe von ungewöhnlichen Lösungswegen auf, die sich schnell als überholt oder nur als Einzelfall herausstellen können. Die Halbwertzeit dieses Arbeitspapier schätze ich als sehr kurz ein.

Auch wenn es nur eine Zwischenbilanz und vor allem keine vollständige Auseinandersetzung mit allen möglichen Formen der IuK-Kriminalität sein kann, war es nötig, die breit verteilten und vereinzelten Erkenntnisse aus 4 ½ Jahren Arbeit am Cyberfahnder zusammen zu fassen. Nur so können sie fruchtbar gemacht werden und die weitere Auseinandersetzung mit dem Thema unterstützen.

Die Resonanz wird zeigen, wo ich falsch liege, welche Fragen unbeantwortet geblieben sind und welche sich neu stellen. Die Cybercrime hat eine beachtliche Dynamik und passt sich allen technischen Entwicklungen und den Nachstellungen der Strafverfolgung an. Das ist kein Grund zum Fatalismus, sondern eine Herausforderung, die es anzunehmen gilt.