# Cybercrime und Strafrecht in der Informations- und Kommunikationstechnik: Cybercrime und Strafrecht in der IuK

Bearbeitet von
Von Dieter Kochheim, Oberstaatsanwalt

*integrieren. Der Markt ist noch jung: Systemübergreifende Standards für die Prüfungen sowie zur systematischen Erfassung der Sicherheitseigenschaften von Apps, auch in Hinblick auf Themen wie mobiles Bezahlen, Home Automation und mobiles Gesundheitsmanagement, müssen sich noch etablieren*. Zwischen 2013 (4. Quartal) und 2016 (1. Quartal) stieg außerdem die Gesamtzahl der Malware-Varianten für Mobilgeräte von gut 3 Millionen auf knapp 9,5 Millionen.[549]

**326** Mit diesen Entwicklungen ist eine hochgradig professionelle Szene entstanden, die das *Skimming* und den Einsatz von Malware als Spitzentechnologie prägt. Dazu gehören die Entwickler von Malware, die Betreiber großer *Botnetze*, der Einsatz von gezielten *DDoS-Angriffen* (klassische Erpressung, Machtkämpfe und Hacktivismus), von Onlinebanking-Malware (*Phishing*) und *Ransomware* sowie die Datenspionage. Unbeachtet gibt es auch Schurkenprovider, die Host- und andere Dienste zur Anonymisierung und Tarnung krimineller Aktivitäten anbieten, und die kommerziellen Betreiber von Exploit-Kits. *Stuxnet* und seine Varianten zeigen, dass es auch militärische Aktivitäten gibt. Auch der noch nicht näher betrachtete Hacktivismus ist symptomatisch dafür, dass destruktive Handlungen auch außerhalb der klassischen kriminellen Szenen zu erwarten sind.

**327** Die Angriffe seit etwa 2014 werden immer gezielter ausgeführt. Beispiele dafür sind die massenhaften Angriffe gegen Rechtsanwälte im Umfeld der Dridex-Gang (Locky) und gegen Institute aus dem Finanzsektor (Anuak, Carbanak), die deutlich machen, dass die Täter auch über umfassendes wirtschaftliches Fachwissen und über praktische Geschäftsabläufe verfügen. Die Meldungen rücken immer häufiger gewerbliche Organisationen in den Vordergrund, die sich Erpressungen und Datenabgriffen ausgesetzt sehen. Die wichtigsten dabei verwendeten Methoden sind nach einer Studie von Verizon aus 2016 geradezu klassisch:[550] Hacking, Malware und Social Engineering. Sie werden nicht mehr breitflächig nach dem Gießkannenprinzip angewendet, sondern sehr gezielt und auf das Angriffssubjekt angepasst (Spear-Phishing). Das Cybercrime bekommt dadurch eine weitere Dimension, die weniger auf eine Breitenwirkung mit vielen Opfern anspricht, die überschaubar geschädigt werden, sondern verstärkt auf einzelne Opfer mit großen Schäden. Jedoch gibt es keine Regel ohne Ausnahmen: 2017 war eine Version des CCleaners, der unter Windows Systemfehler beseitigt und Zwischenspeicher löscht, mit einer Malware verseucht, die sich gezielt gegen *ausgewählte Technik- und Telekommunikationsunternehmen in Japan, Taiwan, Großbritannien, Deutschland und den USA* richtete.[551] Zeitgleich wurde bekannt, dass mehrere Zugangsprovider automatische Updates auf maliziöse Quellen umleiteten, um den betroffenen itS Malware zuzuleiten (Variante von FinFisher).[552] Beide Beispiele zeigen eine gegenläufige Entwicklung, bei der zwar auch eine intensive Vorbereitung auf ausgesuchte Opfer nötig ist, der Angriff selber ohne Mitwirkung des Opfers, sondern mit rein technischen Mitteln erfolgt.

---

[549] McAfee Labs Threat-Report August 2015, 29.8.2015, 31; McAfee Labs, Threat-Report Juni 2016, 9.6.2016, 42.

[550] Uli Ries, Sicherheits-Report: Unternehmen setzen selbst simple Schutzmechanismen nicht um, Heise Security 26.4.2016.

[551] Olivia von Westernhagen, 20 unter 2 Millionen: CCleaner-Malware attackierte große Unternehmen, Heise online 21.9.2017; Olivia von Westernhagen, Axel Vahldiek, Schadsoftware vom Virenschutz-Hersteller. Wochenlang Backdoor in CCleaner, c't 21/2017, 47.

[552] Uli Ries, FinFisher: Internetprovider schieben Spitzelopfern Malware unter, Heise online 21.9.2017.

**328** Seit 2015 beobachtet das BSI verstärkt Erpressungen gegen Unternehmen mit der Drohung mit einem DDoS-Angriff:[553] *Parallel zum Versand der Erpresserschreiben führten die Täter kurze Angriffe durch, um ihre Leistungsfähigkeit zu demonstrieren und die Ernsthaftigkeit der DDoS-Erpressung zu unterstreichen. Gingen die Betroffenen nicht auf die Erpressung ein, kam es zu DDoS-Angriffen durch die beiden Gruppen DD4BC und Armada Collective, bei Kadyrovtsy wurden solche Angriffe hingegen nicht beobachtet. Aufgrund der öffentlichen Berichterstattung traten zudem mehrere Trittbrettfahrer auf den Plan, die ohne tatsächlich durchgeführte DDoS-Angriffe auf eine Zahlung der Empfänger hofften. Das Lösegeld wurde in vielen Fällen in Form der Kryptowährung Bitcoin gefordert*.

**329** Allen voran hat das BSI vor ungesicherten Steuerungsanlagen gewarnt, die unter einer IP-Adresse ohne Zugangsschutz und ohne Firewall und Virenscanner betrieben werden. Leitend war dabei, dass die Steuerung als solche ausfallen und kaskadierende Prozesse in Gang setzen kann. Ein Beispiel für solche Auswirkungen stammt aus 2006: Seinerzeit kollabierte das europäische Stromnetz für die Dauer von zwei Stunden, weil eine einzige Hochspannungsleitung über der Ems planmäßig vom Netz genommen wurde. Am 4.11.2006 schalteten sich wegen Überlastungen binnen 15 Sekunden 14 Schaltstellen des E.ON-Netzes zwischen Niedersachsen und Bayern ab. Die Auswirkungen davon wurden nicht nur in den Nachbarstaaten spürbar, sondern bis nach Kroatien und Nordafrika.[554] Im Jahr davor, im November 2005, fand das *Münsterländer Schneechaos* statt, bei dem nach heftigen Schneefällen etliche Strommasten unter der Schneelast einbrachen und anfangs etwa 250.000 Menschen – davon in mehreren Gemeinden bis zu vier Tagen lang – unter Stromausfall litten.[555] Beide Beispiele zeigen die Anfälligkeit vernetzter Systeme gegenüber Naturkatastrophen und anderen unvorhergesehenen Eingriffen und die dadurch ausgelösten kaskadierenden Effekte. Manipulierte industrielle Steuerungsanlagen könnten ähnliche, wenn nicht noch schwerwiegendere Ausfälle bewirken, wenn die Angriffe punktgenau und skrupellos gegen Kritische Infrastrukturen geführt werden.

**330** Damit verwandt sind die Angriffe über Zugänge für die Fernwartung, über die mehrfach im Zusammenhang mit Telefonanlagen und missbräuchlichen Anrufen zu Mehrwertdiensten oder zu Fernverbindungen berichtet wurde. Ihre mächtigste Ausprägung geht auf den September 2016 zurück und auf das Botnetz unter der Regie der Botware *Mirai*: Es bestand aus mehr als einer Million IoT-Geräten wie Kameras, Haushalts- und Multimediageräten, die allein aufgrund ihrer Menge DDoS-Angriffe mit einer Datenmenge von bis zu 1,1 Terabit pro Sekunde ausführen konnten.[556]

**331** Die duale Welt ist eine technisch vernetzte Welt, in der sich die reale Welt zunehmend auch abhängig von der virtuellen Welt und der Netztechnik als solche macht. Sie erfordert ein neues Nachdenken und nach neuen Konzepten, um sich gegen Ausfälle und Angriffe zu wappnen. Allein Mirai hat gezeigt, dass es eine untere Schwelle für Sicherheitsüberlegungen nicht gibt und selbst „harmlose" Kameras, Kopier- und andere IoT-Geräte zu mächtigen Waffen werden können. Es bedarf neuer Konzepte für die Grundsicherung des Internet-of-Things und die klare Erkenntnis, dass für jede Technik

---

[553] BSI, Die Lage der IT-Sicherheit in Deutschland 2016, 8.11.2016, 29.

[554] BNA, Bericht der BNA über die Systemstörung im deutschen und europäischen Verbundsystem am 4. November 2006, BNA 26.2.2007.

[555] T. Deutschländer, B. Wichura, Das Münsterländer Schneechaos am 1. Adventswochenende 2005, DWD (Deutscher Wetterdienst) 20.4.2015.

[556] Florian Rötzer, Aus dem Internet der Dinge wird eine Armee der Dinge, Telepolis 24.10.2016.

eine Risikoanalyse erforderlich ist, die für jedes gesteigerte Risiko eine entsprechende Absicherung verlangt.[557]

Für das Cybercrime gilt dasselbe, was schon seit Jahrzehnten für die Wirtschafts- **332**
kriminalität und andere besondere Kriminalitätsformen gilt: Sie bewegen sich zum größten Teil außerhalb der Wahrnehmung der Öffentlichkeit und zeigen ihre schädlichen Wirkungen nur vereinzelt. Ihre Täter wiegen sich in Sicherheit, weil sie mit Methoden handeln, die anderen schwer verständlich und womöglich noch schwerer zu entdecken sind. Dadurch fällt es ihnen leicht, Mittäter, Gehilfen und Gefolgsleute zu gewinnen. Ihre Bekämpfung verlangt nach besonderen Anstrengungen in personeller und sachlicher Form. Dazu gehören vor allem Neugierde, Fachwissen und die Gelegenheit, beides zu pflegen.

---

[557] Kapitän Adama hat in irgendeiner, ganz alten Galactica-Folge sinngemäß gesagt: *Die Galactica ist ein Kriegsschiff, sie hat keine vernetzten Computer*. Da ist was dran.

## Kapitel 3. Formen und Methoden des Cybercrime

Das Cybercrime hat verschiedene Quellen, verfolgt verschiedene Ziele und hat ver- **333**
schiedene Umgebungen, die es unterstützen. Ihren Ursprung hat es im **Hacking**, also bei dem Einschleichen und dem Einbruch in fremde informationstechnische Systeme – itS.[558] Das **Social Engineering** liefert Sozialtechniken der Manipulation und Suggestion hinzu. Es dient dazu, frei verfügbare Informationen (Telefonlisten, Baupläne, Presseberichte, wissenschaftliche Publikationen) zu erheben, fachkundig zu bewerten und daraus weiter gehende Schlüsse zu ziehen, menschliche Schwächen zur Informationsbeschaffung, zur Erlangung von Zugangsrechten oder zur Überwindung von Hemmungen auszunutzen (Ausführen von unbekannten Anlagen zu E-Mails, Aufruf präparierter Webseiten) oder sich durch persönliches Auftreten Zugang zu gesicherten Einrichtungen zu verschaffen.[559] Kevin Mitnick:[560] *Social Engineering benutzt Techniken der Beeinflussung und Überredungskunst zur Manipulation oder zur Vortäuschung falscher Tatsachen, über die sich ein Social Engineer eine gefälschte Identität aneignet. Damit kann der Social Engineer andere zu seinem Vorteil ausbeuten, um mit oder ohne Verwendung von technischen Hilfsmitteln an Informationen zu gelangen*.

Der Einsatz von **Malware** beginnt bei den *Rootkits*, mit denen ein Hacker seine **334**
Spuren verwischt, seine Hintertüren für einen ungesicherten Zugang (*Backdoor*) und Veränderungen am angegriffenen System tarnt (*Keylogger*,[561] Fernsteuerungen,[562] *logische Bomben*[563]). Seit dem Auftauchen von *Onlinebanking-Malware* und *Bot Ware* wurden die Mechanismen zunehmend automatisiert, so dass ein menschliches Eingreifen immer seltener nötig ist und die Steuerung der Malware durch einen Command & Control-Server – C & C – erfolgt, der sich zur Tarnung auch weiterer Vorposten (Flux Server[564]) bedienen kann. Im Zusammenhang mit der zunehmend automatisierten Malware unterscheide ich zwischen der **Basis-Malware** und der **produktiven Malware**. Die Basis-Malware hat die Aufgaben, in das fremde itS einzudringen, sich einzunisten und erst dann „produktiv" zu werden.[565] Schon dabei wird sie unterstützt von einem *C & C-Server*, indem sie ihm die Umgebungsvariablen meldet (*Browsertyp*, *Betriebs-*

---

[558] Eindrucksvoll sind die Beispiele bei: Kevin Mitnick, William Simon, Die Kunst des Einbruchs. Risikofaktor IT, mitp 2006.

[559] In seiner Serie Security Journal veröffentlichte McAfee 2008 eine Studie, die sich ausschließlich mit dem Social Engineering befasste. Sie ist leider nicht mehr verfügbar (broken link).

[560] Kevin Mitnick, William Simon, Die Kunst der Täuschung. Risikofaktor Mensch, mitp 2003.

[561] Im engeren Sinne handelt es sich um die automatische Aufzeichnung von Tastatureingaben und im weiteren Sinne auch um die Aufzeichnung von Verarbeitungsprozessen und die Durchsuchung von Dateien (*Spyware*).

[562] Zum Beispiel Bot Ware und Onlinebanking-Malware.

[563] Das sind destruktive Programme, die bei einem Anlass (Zeitpunkt, Umgebungsaktivitäten, durch Fernsteuerung) Einfluss auf das angegriffene System nehmen. Der Begriff wird vor allem im Zusammenhang mit Cyberwar-Strategien verwendet, könnte aber auch Eingang in neue Formen von Erpressungen finden: Wer den Forderungen nicht nachkommt, muss damit rechnen, dass Kühlanlagen, Fahrstühle oder andere Anlagen ausfallen, weil der Erpresser Programme versteckt hat und steuern kann, die genau das bewirken können.

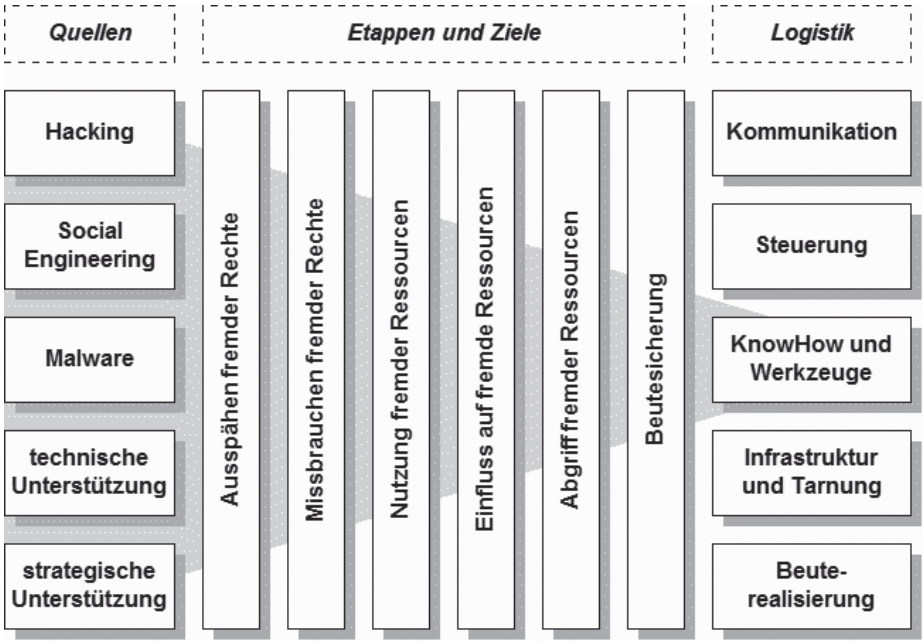
[564] Jürgen Schmidt, Hydra der Moderne. Die neuen Tricks der Spammer und Phisher, c't 18/2007, 76.

[565] *Dieter Kochheim*, Automatisierte Malware. Über das Verschwinden der Cybercrime, April 2012.

*system*, Aktualisierungsstand, IP-Adresse, Tastatur- und Spracheinstellungen) und er ihr die dafür notwendigen *Exploits*, Zusätze, *Updates* und *Rootkits* zur Tarnung zuliefert. Je nach ihrem produktiven Zweck muss die Malware sofort aktiv werden (*Bot Ware*, *Ransomware*) oder sich quasi „schlafen legen und lauschen", um auf bestimmte Umgebungsaktivitäten zu warten (*Onlinebanking-Malware*, *logische Bomben*).

**335** Hinzu gekommen sind die **kriminellen Dienstleister**. Dabei handelt es sich einerseits um Einzelpersonen, die Zugangs- und Zahlungskartendaten, Exploits, Rootkits, Malware oder Infrastruktur feilbieten und zuliefern oder schlicht Kontakte vermitteln. Der Übergang zu *Operating Groups* ist fließend. Bei ihnen handelt es sich um arbeitsteilige Gruppen, die sich dauerhaft verbinden, um Projekte mit langzeitiger Ausrichtung (Malware-Entwicklung, Programmpflege) oder mit spezialisierter Ausrichtung (Übersetzungsdienste, Programm- und Webshoppflege, Beutesicherung) auszuführen. Andererseits können – noch selten – bandenartige Gruppen festgestellt werden, die mit infrastrukturellem Aufwand spezialisierte Boards, Bullet Proof- und Infiltrationsdienste (Crimeware-as-a-Service) für andere anbieten oder dauerhaft auch Botnetze, Ransomware oder das automatisierte Phishing betreiben.

**336 Strukturmodell zum Cybercrime**




*Grafik: Strukturmodell zum Cybercrime*

**337** In den Vordergrund ist das *strategische Hacking*, also der Einsatz von Malware getreten. Das zeigen vor allem die beschriebenen → Spionage-Operationen *Shady Rat*, *Aurora* und *Night Dragon*, an deren Anfängen zwar die intellektuelle Auswahl von Angriffszielen stand, aber der erste Angriff – sozusagen als Perforation – durch autonome Basis-Malware erfolgte, die keine oder kaum noch menschliche Steuerungen benötigte.

Erst als die *Backdoor* geschaffen und das angegriffene System perforiert war, griffen die menschlichen Angreifer wieder ein und übernahmen den produktiven Angriff. Nur *Stuxnet* und seine Varianten sind für den völlig autonomen Einsatz vorgesehen, was sie zu etwas Besonderem macht.

Die technischen und strategischen Unterstützungen, die als „Quellen" in der Grafik **338** aufgeführt sind, spielen inzwischen eine nachhaltige Rolle, wie die *Bullet Proof-Dienste* und die Anbieter der *Crimeware-as-a-Service* belegen. Sie vermarkten anonymisierte Netzdienste und die ganze lästige Infrastruktur, um Malware und Ransomware zu betreiben oder Botnetze einzurichten. Unter dem technischen Aspekt sind *Terminals*, *Proxys* und *Anonymisierer* (kaskadierende Zugriffssysteme, zum Beispiel TOR[566]) bedeutsam für die Tarnung des Angreifers, anonymisierte Hostspeicher (*Drops*) und C & C-Server nötig für die Durchführung und Beutesicherung. Als strategische Unterstützung wirken vor allem geschlossene Kommunikationsplattformen, *Operating Groups* und Geldgeber (*Koordinatoren*), aber auch Auftraggeber und Unterstützer mit politischen oder wirtschaftlichen Motiven. Das Mittelfeld der Grafik bilden die „Etappen und Ziele". Sie beschreiben die Eingriffstiefe, bis zu der die einzelnen Formen des Cybercrime vordringen – unabhängig davon, aus welcher Quelle sie stammen und in welcher Kombination sie dabei auftreten. Der Zugriff auf fremde itS bedeutet zunächst nichts anderes, als Zugangsrechte zu erforschen und zum Zugang zu nutzen. Die Nutzung fremder Ressourcen bedeutet das Ausspähen geschützter Informationen, ihre Nutzung und schließlich die Manipulation des angegriffenen itS (*Backdoors*, *Installationen*, Veränderungen der Funktionalität). Der Abgriff von Ressourcen reicht vom „Diebstahl" von rechnerischen Kapazitäten bis zum funktionalen Missbrauch (Onlinebanking, Funktionsänderung, Nutzung als *Zombie*). Die Beutesicherung besteht schließlich darin, außerhalb des angegriffenen itS Nutzen aus dem Angriff zu ziehen.

An dieser Stelle greifen die Funktionen, die in der Grafik als „Logistik" bezeichnet **339** werden. Unter „Kommunikation" verstehe ich die Boards, Foren und Hosts für *Drops*, unter denen gestohlene Informationen gesammelt und verteilt werden. Sie liefern die Marktplätze für die vorbereitenden Informationen, zum Tausch von Knowhow, Exploits und Kontakten und schließlich zum Handel mit der virtuellen Beute. Die weiteren Merkposten betreffen die Leistungen, die von *Schurkenprovidern* als Services bereitgestellt werden (vor allem Tarnung und Anonymität) und der Verbreitungsdienste (*Crimeware-as-a-Service*). Nahtlos reiht sich dazu die „Beuterealisierung" ein, die zum Beispiel die Anbieter von *Mule Accounts* (*Bankdrops*), Inkassodiensten und Wechselstuben zwischen verschiedenen Bezahlsystemen umfasst.

Während die **Geschichte des Cybercrime** das Nebeneinander der technischen, wirt- **340** schaftlichen und schließlich kriminellen Erscheinungsformen in den Blick genommen hat, geht es jetzt um die Erscheinungsformen selber und ihren Wandlungen. Dazu müssen bereits einzelne Rechtsfragen angesprochen werden, soweit das zum Verständnis erforderlich ist. Die vertiefte Auseinandersetzung mit dem materiellen IuK-Strafrecht erfolgt im → *Teil 2*.

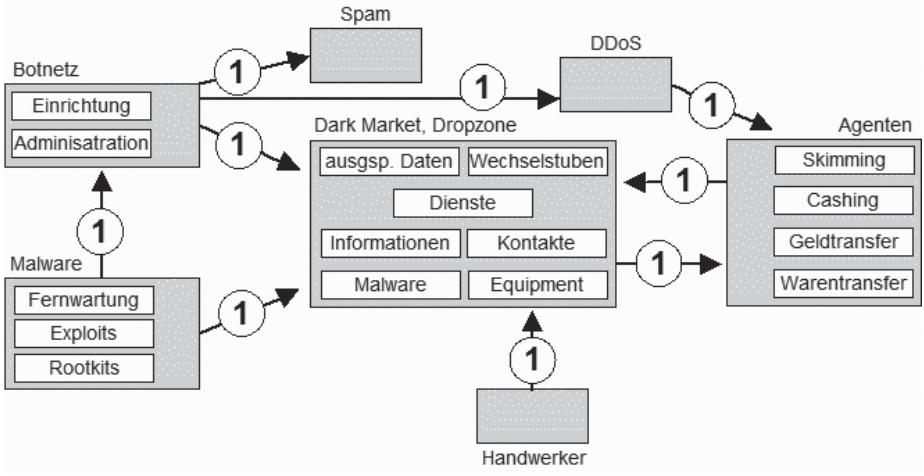
Die organisierten Erscheinungsformen des Cybercrime, allen voran das Skimming, **341** der Betrieb von Botnetzen, das Phishing und die Crimeware-Dienste, sind noch eher Ausnahmeerscheinungen. Für die meisten Erscheinungsformen ist es realistischer, von einer marktartigen Tauschgesellschaft auszugehen, in der vorwiegend Einzelpersonen

---

[566] Bei der Nutzung von Anonymisierern wird eine Anfrage ins Internet nicht direkt an den Host gestellt (Speicherplatz für Inhalte), sondern über eine Kette von Servern, die nur ihren jeweiligen „Nachbarn" kennen und das Ergebnis über dieselbe Kette zurück melden (The Onion Router).

und allenfalls kleine Verbünde (*Operating Groups*) handeln und in der jeder an jedem verdient.

### 342 Arbeitsteiliges Cybercrime[567]




*Grafik: Arbeitsteiliges Cybercrime*

## A. Schema eines Hacking-Angriffs[568]

**343** Schon die KGB-Hacker von 1985 schürften nach werthaltigen Informationen. Das machen die modernen und aufgerüsteten Spionage-Operationen auch, wobei sie jetzt Malware zur Perforation des Angriffsziels und hoch entwickelte Tarnungen einsetzen können (*Rootkits*).

**344** Um die Eignung eines Angriffsziels abschätzen zu können, muss es technisch, möglichst auch geographisch lokalisiert und wegen seiner sachlichen Eignung beurteilt werden (*Footprinting*).[569] Der erste Schritt besteht häufig in dem Ausloten, ob überhaupt ein Zugang besteht, mit einem *Ping* (Messung der Erreichbarkeit einer Netzwerkadresse und im weiteren Sinne eines ihrer Zugangskonten, wenn der Zugang durch Zugangsdaten gesichert ist). Mit weiteren Messinstrumenten lassen sich zusätzliche, öffentliche In-

---

[567] Die Kreise mit der Ziffer 1 kennzeichnen Bezahlvorgänge (Sinnbild für eine Münze). Dem Modell fehlen noch die *Crimeware-as-a-Service*-Dienste, die die komplette infrastrukturelle Umgebung für die Verbreitung und die Pflege von Malware schaffen und über die gesamte Breite der Grafik tätig sind, ohne die produktiven maliziösen Projekte selber auszuführen, nachdem sie mit kriminellen Methoden die Voraussetzungen für die Installation der produktiven Malware geschaffen haben und die Infrastruktur dafür zur Verfügung stellen, um die Betriebsbereitschaft der produktiven Malware auf der infrastrukturellen – nicht administrativen – Ebene zu gewährleisten.

[568] Zu den Methoden des Hackings und des Social Engineerings: Kevin Mitnick, Wiliam Simon, Die Kunst des Einbruchs (2005), Heidelberg 2006; dieselben, Die Kunst der Täuschung (2002), Heidelberg 2003. Zur Funktionsweise von Malware: Tatort Internet – die c't-Serie.

[569] Dasselbe Vorgehen beschreibt Steffens im Zusammenhang mit Spionage-Angriffen gegen Unternehmen und Behörden: Timo Steffens, Hacker-Jagd im Cyberspace. Grundlagen und Grenzen der Suche nach den Tätern, c't 14/2017, 122, 123.