Bundeskriminalamt

Täter im Bereich Cybercrime

Eine Literaturanalyse

Teil I – Eine phänomenologische und tätertypologische Betrachtung

Teil II – Kriminologische Erklärungen und Handlungsmöglichkeiten

Stand: 04.12.2015

Bundeskriminalamt
Kriminalistisches Institut
Forschungs- und Beratungsstelle Cybercrime KI 16

BKA

Jörg Bässmann
KI 16-Forschungs- und Beratungsstelle Cybercrime
Bundeskriminalamt
65173 Wiesbaden
KI16@bka.bund.de

Inhaltsverzeichnis

Verzeichnis der Tabellen:

Verzeichnis der Abbildungen:

Zusammenfassung

Täter in der Cyberkriminalität bzw. Cybercrime im engeren Sinne werden häufig relativ undifferenziert als „Hacker“ bezeichnet. Dabei stellt sich wie in anderen Kriminalitätsbereichen auch die Frage, inwieweit eine Differenzierung unterschiedlicher Tätertypen ggf. auch differenzierte staatliche Antworten auf diese Täter ermöglichen würde.

In nachfolgendem Bericht wurde die deutsch- und englischsprachige Literatur ab dem Jahr 2000 zum Thema Cybercrime im engeren Sinne auf täterspezifische Erkenntnisse ausgewertet. Der Zugang zu den Medien erfolgte in erster Linie netzbasiert über das Internet, über Extrapol sowie über das Intranet des BKA. Die Arbeit hatte mit der Schwierigkeit zu kämpfen, dass es bislang kaum nach hohen wissenschaftlichen Standards durchgeführte kriminologische Untersuchungen zur Thematik gibt.

In phänomenologischer Hinsicht zeigt der Bericht, dass der typische Hacker Schüler, Auszubildender oder Student ist, der seine Kenntnisse im Bereich Informationstechnik häufig als Autodidakt erworben hat. Das ist heute einfacher als früher, sind viele junge Hacker doch als sog. „digital natives“ mit Computern und dem Internet als Informationsplattform groß geworden. Die meisten Hacker verbringen ihre Freizeit vor allem mit dem Computer und arbeiten viel alleine, ohne dabei sozial auffällig zu sein. Sie unterhalten eher informelle Kontakte, die offenbar eher dem Augenblick als einer soliden Einbindung in soziale Strukturen bzw. Gruppen entstammen. Kontakte werden vor allem über Chats, Cliquen oder als individuelle Freundschaften auch in der realen Welt gepflegt.

Für das Handeln von Hackern scheinen weniger Einzelmotive als Motivbündel ausschlaggebend zu sein. Relevanz haben insbesondere der Spaß am Hacken, Neugier und Unterhaltungsaspekte, genauso wie der Nervenkitzel dabei, etwas Unerlaubtes zu tun. Das Streben zu einer Gruppe Gleichgesinnter zu gehören und durch das Handeln an Achtung und Anerkennung sowie an Status in der eigenen Gruppe bzw. Community zu gewinnen, sind ebenfalls relevante Antriebsgründe, genauso wie der scheinbare Erwerb von Macht durch die Kontrolle fremder Systeme. Darüber hinaus dürfen monetäre und politische Gründe als Anreize für Hacker genauso wenig vergessen werden, wie das Streben nach Zerstörung oder Rache. Im Zusammenhang mit der intrinsischen Motivation zum Hacken wird gerade für qualifizierte Hacker das Erleben von flow-Erfahrungen berichtet, wie sie auch aus Risikosportarten bekannt sind.

Um erfolgreich in fremde Computer und Netzwerke einzudringen, ist nicht mehr zwingend ein hohes Fertigkeitsniveau im IT-Bereich notwendig. Im Netz verfügbare Angebote von „Crime as a Service“ oder „Malware as a Service“ machen es auch weniger geübten Tätern möglich, Angriffe auf Computer und Netzwerke zu verüben. Die Angriffsziele sind dabei vielfältig. Abhängig insbesondere auch von der jeweiligen Motivation werden Firmen jedweder Größe, Webseiten von Regierungen und Verwaltungen, Pornoseiten, ethnische oder religiöse Webseiten, Banksysteme oder auch die Webseiten von Privatleuten attackiert.

Die wenigsten Cyberstraftäter scheinen bereits mit dem Strafjustizsystem in Berührung gekommen zu sein. Mögliche Strafen oder auch Haft sind praktisch ohne Abschreckungswirkung, werden die Kompetenzen und Möglichkeiten der

Strafverfolgungsseite doch als nicht besonders hoch eingeschätzt. Eine Rolle dürfte dabei auch die Möglichkeit spielen, infolge der vorhandenen Qualifikationen trotz Straffälligkeit noch Karriere im IT-Sektor machen zu können, wie Hackerlegenden beispielhaft zeigen.

Im Hinblick auf den Kernauftrag, Möglichkeiten der Tätertypisierung zu erkunden, zeigt der Bericht, dass Hacker in den letzten 25 Jahren vorrangig nach ihrem Fertigkeitsniveau, dem Zweck bzw. der Motivation ihres Handelns und in neuerer Zeit auch nach ihrer beruflichen Herkunft bzw. ihrem Auftraggeber typisiert worden sind. Regelmäßig finden mehrere dieser Faktoren gleichzeitig Berücksichtigung. Hinweise zur methodischen Herangehensweise an die Entwicklung von Tätertypen im Bereich Hacking fanden sich in der Literatur kaum. Eine tiefergehende methodische Analyse der Typenbildungen von Hackern war insofern im Rahmen dieser Literaturerhebung nicht möglich.

Die Arbeit liefert dennoch nicht nur einen chronologischen Überblick über Typenbildungen bei Hackern, sondern gibt auch einen Überblick in der Breite, der von eher groben Differenzierungen nach dem Fertigkeitsniveau bis hin zu komplexen Typendifferenzierungen insbesondere auch unter motivationalen Aspekten reicht. In den meisten Typensystemen spielten übrigens beide Aspekte eine Rolle. Neuere Typisierungen referenzieren zudem auf die Herkunft bzw. die institutionelle Zuordnung von Hackern, wie das am Beispiel der Typenbildung des niederländischen National Cyber Security Centre deutlich wird. Basierend auf einem an die Literatur angelehnten Modell von Hackertypen wird in jährlichen Lageberichten eine typenspezifische Gefährdung als Ausgangspunkt für nationalstaatliche Gegenstrategien u. a. zur Stärkung der Resilienz in unterschiedlichsten Bereichen beschrieben.

In kriminologischer Hinsicht hat sich die Studie den im Zusammenhang mit Cybercrime am häufigsten genannten kriminologischen Theorien zugewandt und ihre Anwendbarkeit geprüft. Im Detail thematisiert der Bericht Bindungs- und Kontrolltheorien, Lerntheorien, die Neutralisationstheorie, die Theorie der rationalen Wahl sowie die Routine-Aktivitätstheorie, die Theorie der Kriminalität als „verbotene Frucht“, die Flow-Theorie und als neue Theorie zur Erklärung von Cybercrime die „Space Transition Theory“. Auch wenn die Theorien für sich allein keine isoliert anwendbaren Erklärungen für Cybercrime im engeren Sinne liefern können, sind sie theorieübergreifend doch von erheblicher Bedeutung nicht nur für die Präventionsarbeit.

In polizeipraktischer Hinsicht ist die Literaturanalyse genutzt worden, um Ideen für täterbezogene Interventionen bzw. Präventionsmaßnahmen zu gewinnen. Ein erfolgversprechender Weg könnte sein, die Repression vor allem auf die relativ kleine Gruppe hochqualifizierter, kreativer Hacker zu konzentrieren, anstatt sich auf die breite Masse an „script-kiddies“ bzw. angelernten Hackern zu fokussieren, die im Wesentlichen vorgefertigte Werkzeuge nutzen. Die Konzentration der Strafverfolgung auf versierte Hacker dürfte auch deshalb gewinnbringend sein, sind sie doch nicht allein die Entwickler immer neuer Angriffswerkzeuge, sondern zugleich auch wichtige Knoten in der täterbezogenen Zusammenarbeit und wichtige Stützen in der Wissensvermittlung für weniger fachkundige Hacker.

Bezüglich der „script-kiddies“ ist nicht auszuschließen, hier ggf. lediglich mit einem neuen Phänomen der Jugenddelinquenz konfrontiert zu sein. Auch deshalb erscheint es sinnvoll, auf soziale Präventionsansätze zu setzen, zu denen – um nur ein Beispiel zu setzen – auf das

Hackingphänomen angepasste Gefährderansprachen zu zählen sind.

In präventiver Hinsicht sprechen die Ergebnisse der Literaturanalyse darüber hinaus für eine Anwendung situativer Präventionsansätze, deren Wirkung in eher klassischen Kriminalitätsbereichen ausreichend belegt ist. Situative Maßnahmen sind in der Regel nicht geeignet, hochprofessionelle und -motivierte Täter von ihrem Tun abzuhalten. Sie sind jedoch ein wirksames Werkzeug für die Masse opportunistischer Täter bzw. derjenigen Täter, die lediglich Tatgelegenheiten nutzen. Bezogen auf das Thema Hacking wären dies diejenigen häufig jugendlichen Täter, die vorgefertigte Angriffswerkzeuge nutzen, weil sie selber über zu wenig Wissen und (finanzielle) Möglichkeiten verfügen, komplexe Angriffswerkzeuge selber zu entwickeln. Situative Ansätze beziehen sich dabei nicht nur auf Maßnahmen der IT-Grundsicherung auf Anwenderseite, sondern lassen sich auch in Täterrichtung einsetzen, um zum Beispiel Möglichkeiten der Neutralisierung von Schuld zu verhindern.

Der Bericht ist am Ende auch Beleg für das insbesondere deutschsprachige Forschungsdefizit, das aus Perspektive der kriminalistisch-kriminologischen Forschung zum Thema besteht.

Summary

Perpetrators in cyber-crime in general and in the narrower sense are frequently referred to indiscriminately as “hackers”. As in other fields of crime, this also raises the question concerning the extent to which a differentiation of offender types might also give rise to differentiated answers by the state in dealing with such perpetrators.

In this report, German and English-language literature starting in the year 2000 on the subject of cyber-crime in the narrower sense was evaluated for offender-specific findings. Access to the media primarily was network-based via the Internet, Extrapol as well as the BKA Intranet. One of the difficulties faced with this work is that hardly any criminological studies in conformity with high scientific standards have ever been carried out in this field.

In phenomenological terms, the report shows that typical hackers are pupils, apprentices or students who have frequently acquired their knowledge of information technology by autodidactic means. Today this is simpler than in the past, seeing as many young hackers have meanwhile grown up as so-called “digital natives”, fully familiar with computers and the Internet as an information platform. Most hackers spend their leisure time especially with computers and work a great deal on their own without being “socially conspicuous”[1] in the process. They tend to maintain informal contacts evidently derived from momentary experiences rather than from solid integration into social structures and groups. Contacts are maintained especially via chats, cliques or also as individual friendships in the real world.

For the actions of hackers, individual motives appear to be less decisive than aggregations of motives. Things of particular relevance are the fact that hacking is fun, followed by curiosity and entertainment aspects as well as the exciting thrill of doing something that is prohibited. Striving to become part of a group of persons with shared interests and to acquire respect, recognition and status in a person’s own group or community likewise are relevant motives, as is the apparent acquisition of power due to the ability to control extraneous systems. In addition, monetary and political reasons should not be ignored as incentives for hackers, just as striving for destruction or revenge may be a conceivable motive. In connection with the intrinsic motivation to engage in hacking, there are manifestations of flow experiences of the kind known from high-risk sports, especially for qualified hackers.

In order to successfully gain access to others’ computers and networks, a high level of IT expertise and skills is no longer imperative. Offerings available on the web, such as “crime as a service” or “malware as a service” also enable offenders with less practice to carry out attacks on computers and networks. In this context, the targets are many and various. Depending in particular on the motivation in each case, attacks are launched on companies of any size, on websites of governments and administrations, pornographic pages, ethnic or religious websites, banking systems and also on web pages of private individuals.

Extremely few cybercriminals appear to have already come into contact with the criminal justice system. Possible forms or punishment or also imprisonment are practically without any deterring effect, seeing as the expertise and resources of the criminal prosecution authorities

[1] Translator’s note: A term in German that can mean, *inter alia*, being maladjusted, non-conformist or lacking in social skills

are not assessed as particularly high. The possibility of embarking on a successful career in the IT sector thanks to the qualifications acquired (even though illegality was involved) also plays a role, as a number of hacker legends have shown in the past.

Considering the core mandate of identifying possibilities for creating offender profiles, the report shows that in the past 25 years, hackers have predominantly been typified according to their level of skills, the purpose of and/or motivation behind their actions and, more recently, also according to their occupational origins and/or principals or employers. A number of such factors are simultaneously taken into account on a regular basis. Hardly any indications were available in literature concerning the methodical approach used in developing offender types in the field of hacking. A more profound methodical analysis of type manifestations amongst hackers thus was not possible within the scope of this literature study.

Nevertheless, not only does the work performed provide a chronological overview of type characterisations amongst hackers; it also facilitates an overview in a certain bandwidth ranging from rather rough differentiations according to the level of skills all the way through to complex type differentiations, in particular also according to motivational aspects. Incidentally, both aspects played a part in most typifying systems. Moreover, new typifying activities refer to the origin and/or institutional "classification" of hackers, as illustrated by the example of typifying activities of the Dutch National Cyber Security Centre. Based on a model of hacker types derived from literature, in annual situation reports a type-specific danger is described as the starting point for national state counterstrategies, *inter alia* to reinforce the resilience in many and various fields.

In criminological terms, the study deals with the criminological theories mentioned most frequently in connection with cyber-crime and their applicability. In detail, the report deals with such topics as attachment and control theories, learning theories, the neutralisation theory, the theory of rational selection as well as the routine activity theory, the theory of criminality as "forbidden fruit", the flow theory and, as a new theory to explain cyber-crime, the "space transition theory". Even if the theories alone cannot provide any explanations for cyber-crime in the narrower sense that can be applied in isolation, they certainly are of substantial significance above and beyond the various theories, not only for preventive work.

In terms of practical police work, the literature analysis has been used in order to obtain ideas for offender-related interventions and/or preventive measures. A promising approach could be to concentrate repression above all on the relatively small group of highly qualified hackers rather than focusing on a broad mass of "script kiddies" or hackers with rudimentary training who essentially use prefabricated tools. The concentration of public prosecution on well-versed hackers is also likely to be beneficial as they are not the developers of an ever new range of attack tools alone but simultaneously represent key nodes in offender-related cooperation and key supports in providing know-how to hackers with less expertise.

With regard to the "script kiddies", it cannot be ruled out that we are merely confronted with a new phenomenon of juvenile delinquency. For this reason too, it appears to be sensible to rely on social prevention approaches that – to name but one – include also police-related deterrent measures towards potential offenders such as warning visits or letters.

Moreover, in preventive terms the findings of the literature analysis argue in favour of applying situation-related preventive approaches whose effectiveness is adequately documented in rather classical fields of criminal investigation. As a rule, situation-related measures are not suitable to deter highly professional and highly motivated offenders from

committing their criminal acts. However, they are an effective tool for the mass of opportunistic perpetrators or those offenders who simply take advantage of any opportunities to commit a crime. In relation to the subject of hacking, these would be those frequently juvenile offenders who use prefabricated tools for attacks because they themselves have too little expertise and too limited (financial) resources to develop complex attack tools themselves. In this context, situation-related approaches do not only refer to measures of basic IT security on the user side but can also be deployed towards offenders so as to prevent possibilities of guilt being neutralised.

Finally, the report also documents the shortfall in research – particular in German – that exists on the subject from the perspective of criminalist and criminological research.

Teil I – Eine phänomenologische und tätertypologische Betrachtung

1 Einleitung

Betrachtet man das Phänomen der Computerkriminalität, alternativ werden Begriffe wie Internet-, Cyberkriminalität oder auch Cybercrime gebraucht, findet sich täterseitig häufig die sehr weite und auch undifferenzierte Täterumschreibung „Hacker“. Ausgehend vom Gedanken einer möglichst wirksamen täterorientierten Intervention wie Prävention stellt sich dem aufmerksamen Betrachter fast zwangsläufig die Frage, ob die Verwendung eines derart oberflächlichen Begriffs für zum Teil recht unterschiedliche Täter bzw. Tätertypen sinnvoll ist. Man könnte an dieser Stelle natürlich entgegnen, dass es für die Polizei völlig unerheblich sei, ob die Rede von „Hackern“ oder „Crackern“, von „Script-kiddies“ oder von „Cybervandalen“ ist. Wichtiger für ihr Handeln bzw. ihre Befugnisse seien juristische Zuschreibungen wie „Täter“ und „Teilnehmer“, „Verdächtiger“ oder „Beschuldigter“.

In diesem Kontext sei angemerkt, dass der Fokus der IT-Sicherheitsindustrie auf die Cyberkriminalität im Kern ein technischer ist (Yip et al., 2012). Ein solcher Ansatz beinhaltet das Risiko, zu einem niemals endenden Katz-und-Maus-Spiel zu führen, in dem neue Technologien auftauchen, Cyberkriminelle sich dieser annehmen und darauf zu reagieren ist. Es wird insoweit empfohlen, Cyberkriminalität als sozio-technologisches Phänomen aufzufassen und auf dieser Ebene auch zu versuchen, die Täter in ihren Eigenarten, ihre Motivationen, Haltungen, ihr Verhalten und die Umgebungen aus denen heraus sie agieren zu verstehen. Einem solchen Ansatz folgt auch diese Arbeit.

Aus eher klassischen Kriminalitätsfeldern ist schon lange bekannt, welchen Wert kriminologisch fundierte Täterklassifikationen beispielsweise im Bereich der Ressourcenallokation haben können. Exemplarisch sei hier auf Franz von Liszt verwiesen, der bereits Anfang des 20. Jahrhunderts Tätertypen im Hinblick auf ihre Rückfallgefährdung klassifiziert und passend dazu Reaktionsmodi mit dem Ziele der Rückfallverhinderung aufgezeigt hat (v. Liszt, 1905). Wir wissen allerdings auch um die Gefahren der Typologisierung. Kategorien von Tätertypen sollten daher allenfalls als Orientierung genutzt werden, lassen sich Menschen doch nur selten präzise irgendwelchen Kategorien zuordnen.

Empirisch begründete Tätertypenbildungen (vgl. dazu Kluge, 2000) sind auch für die Polizeiarbeit nichts grundlegend Neues und werden genutzt, um eine möglichst wirkungsvolle wie Ressourcen schonende täterorientierte Arbeit zu ermöglichen. Ein Beispiel ist die Gruppe der jugendlichen „Mehrfach- und Intensivtäter“, die von den Polizeien der Länder im Wesentlichen auf der Basis der Anzahl und der Schwere der von ihnen in einem festgelegten Zeitraum begangenen Straftaten klassifiziert werden, um auf dieser Basis mit polizeilichen Maßnahmen unterschiedlicher Intensität behandelt werden zu können (BKA, 2012). Jedem polizeilichen Jugendsachbearbeiter bekannte Begriffe sind hier die des Einmal-, Schwellen-, Mehrfach- und Intensivtäters. Auch wenn in den Ländern zum Teil leicht divergierend Definitionen zu diesen Begrifflichkeiten existieren und auch nicht alle Begriffsspezifikationen in allen Bundesländern Verwendung finden mögen, bietet die Grundeinteilung doch ein polizeilich anerkanntes Unterscheidungssystem.

Täterprofile und -klassifikationen finden sich auch in anderen klassischen Kriminalitätsfeldern wie bspw. dem Einbruchsdiebstahl. Hier haben nach wissenschaftlichen Standards durchgeführte Täterbefragungen Erkenntnisse u. a. zur Motivation, Tatortauswahl, Kosten-Nutzen-Abwägungen, Planungsverhalten und Modi Operandi aufzeigen können, die in der Gesamtschau mit anderen Erkenntnisquellen wichtige Ansätze für eine wirkungsvolle Prävention liefern können (Feltes, 2004). Von besonderer Bedeutung ist die Täterorientierung jedoch im Bereich der Korruption, einem „opferlosen" Delikt, das insbesondere über täterorientierte Maßnahmen beeinflussbar ist, wie die im BKA getroffenen Maßnahmen zur Korruptionsprävention anschaulich zeigen.

Während es also in den klassischen Kriminalitätsphänomenen der Jugend-, Gewalt-, Sexualdelinquenz oder auch der Betrugsstraftaten eine zum Teil breite Auswahl täterorientierter Untersuchungen und Literatur (bspw. zu Erklärungsansätzen und Karriereverläufen) gibt, erscheint das Feld in dem noch relativ jungen Bereich „Cybercrime" noch weitestgehend unbestellt.

Der nachfolgende Bericht arbeitet das Thema mittels einer Analyse der seit dem Jahre 2000 veröffentlichten deutsch- und englischsprachigen Literatur auf. Frühere Arbeiten wurden lediglich ausnahmsweise berücksichtigt. Neben Ressourcenaspekten sprach dafür, dass es sich bei dem hier bearbeiteten Forschungsfeld noch um ein relativ junges handelt, das sich zugleich in einem Zustand permanenter Umwälzung befindet, der sich natürlich auch auf täterbezogene Phänotypen auswirkt. Um nur ein Beispiel zu nennen: In der älteren Literatur findet sich regelmäßig der Hinweis auf sog. „phreaker", d. h. Hacker, denen es gelang, durch die Manipulation analoger Telefonverbindungen kostenlos zu telefonieren (Hafner und Markoff, 1992; Kempa, 2006). Dieses Phänomen spielt in der heutigen Zeit digitaler Telefon(verbindungen) praktisch keine Rolle mehr und ist damit für diese Arbeit irrelevant. Auf der anderen Seite scheinen die größten Gefahren für die Informations- und Kommunikationstechnologie, die wiederum für moderne Gesellschaften immer bedeutender werden, vgl. z. B. die Industrie 4.0 oder das Internet der Dinge, heute nicht mehr von technikbegeisterten Hackern als Einzeltätern, sondern von organisierten Gruppen und auch von Staaten auszugehen. Diese beiden beispielhaft genannten Themen wiederum erschienen zu Beginn dieses Jahrtausends noch völlig irrelevant.

In Teil I dieses Berichts wird in den nachfolgenden Kapiteln zunächst der dem Projekt zugrunde liegende Auftrag wiedergegeben, bevor die angewandte Methodik erläutert wird. Es folgt eine für eine Typenbildung notwendige phänomenologische Beschreibung der Literaturerkenntnisse zu Cybercrimetätern, bevor in der Literatur genannte Hacker-Typenbildungen erläutert werden.

Zur Abrundung und zugleich um das aus der Literatur gewonnene Wissen für die weitere Diskussion des Themas möglichst umfassend zur Verfügung zu stellen, werden nachfolgend in einem Teil II die wesentlichen in der Literatur aufgeführten kriminologischen Erklärungen für das Hacking beschrieben, bevor die Arbeit mit der Darstellung von Literaturerkenntnissen zu täterspezifischen Handlungsmöglichkeiten und einer Ergebniszusammenfassung endet.

2 Auftrag / Ziel

Basis für diese Arbeit ist ein Auftrag der Abteilungsleitung des Kriminalistischen Instituts gewesen, die deutsch- und englischsprachige Literatur seit der Jahrtausendwende zum Thema

Cybercrime im engeren Sinne auf täterspezifische Erkenntnisse auszuwerten. Dabei geht es in erster Linie um die Beschreibung unterschiedlicher Tätertypen bzw. die Analyse vorhandener Tätertypologien. Auch wenn es nicht gerade trivial ist zu erkennen, welcher Akteur für einen Cybersicherheitsvorfall verantwortlich ist (vgl. National Cyber Security Centre, 2012), erscheint eine Analyse des Wissens über Täter, ihre Taten, Motivationen und Rechtfertigungen sowie eine darauf aufbauende Klassifizierung von Tätertypen doch grundsätzlich geeignet, nicht nur den kriminologischen Diskurs zu befördern, sondern in ganz praktischer Hinsicht zielgruppenorientierte Interventions- und Präventionsstrategien für unterschiedliche Tätergruppen zu entwickeln.

Im Einzelnen sollten in dieser Sekundäranalyse daher

- deutsch- und englischsprachige Literatur seit der Jahrtausendwende auf Tätertypen und Tätertypologien zum Thema Cybercrime im engeren Sinne (zum Begriff siehe Ausführungen unten) ausgewertet werden,
- vorhandene Tätertypen und Typologien beschrieben, möglichst verglichen und im Hinblick auf die Anwendbarkeit in der (polizeilichen) Praxis auch bewertet werden,
- ggf. bereits vorhandene Ansätze der (polizeilichen) Herangehensweise an unterschiedliche Tätertypen ausgewertet und
- Aspekte der Karriereforschung berücksichtigt werden. So stellt sich die Frage, ob bzw. inwieweit sich Erkenntnisse aus traditionellen Kriminalitätsbereichen auf den Bereich der Cybercrime übertragen lassen.

Aufgabe war es nicht, das Täterhandeln in eher klassischen Kriminalitätsbereichen wie dem Betrug (der als Waren- oder Warenkreditbetrug heutzutage häufig im Internet bzw. auf Online-Marktplätzen stattfindet) der Beleidigung oder Verleumdung (beispielsweise in sozialen Netzwerken) zu untersuchen, sondern sich auf die sog. Cybercrime im engeren Sinne zu beschränken. Darunter werden lediglich diejenigen Straftaten verstanden, die sich gegen das Internet, Datennetze, informationstechnische Systeme oder deren Daten richten (Bundeskriminalamt, 2014). Diese Kriminalitätsform wird im Deutschen z. T. auch „technikorientierte Cybercrime“ (Brodowski und Freiling, 2011) und im Englischen treffend „Cyber-dependent crimes“ genannt (McGuire und Dowling, 2013a). In Deutschland werden davon gemäß Bundeslagebild 2013 (Bundeskriminalamt, 2014) folgende Delikte umfasst: Computerbetrug nach § 263a StGB, Betrug mit Zugangsberechtigungen zu Kommunikationsdiensten, Fälschung beweiserheblicher Daten gemäß § 269 StGB, Täuschung im Rechtsverkehr bei Datenverarbeitung gemäß § 270 StGB, Datenveränderung gemäß § 303a StGB, Computersabotage gemäß § 303b StGB sowie Ausspähen und Abfangen von Daten einschließlich Vorbereitungshandlungen gemäß §§ 202a, 202b, 202c StGB.

Der Bericht geht damit nicht auf Pornographiedelikte (u. a. mit Kinder- und Jugendpornographie) ein, geht es hier doch im Kern um die „bloße“ Verbreitung inkriminierter Inhalte. Ebenfalls nur ansatzweise thematisiert werden Pirateriedelikte und damit strafbewehrte Schutzrechtsverletzungen (Meier, 2012). Beide Themen werden regelmäßig der Cybercrime zugerechnet (vgl. Europarat, 2001). Während Pornographiedelikte dabei vor allem für das Dilemma stehen, dass klassische Kriminalitätsfelder zunehmend von modernsten Technologien durchdrungen sind und Polizei und Staatsanwaltschaft damit vor

immer größere Herausforderungen gestellt werden, ist im Bereich der Pirateriedelikte zu trennen zwischen dem Massenphänomen der Gelegenheitskopierer (zum Begriff vgl. Krömer und Senn, 2011), die ohne dass sie tiefergehende Computerkenntnisse besitzen müssen im Internet verfügbare Tauschbörsen nutzen und organisierten Raubkopierern („Release-Szene“). Allenfalls letztere Gruppe hat Relevanz für diesen Bericht (vgl. Kapitel 5.3.2).

Abgrenzungsschwierigkeiten bereiteten organisierte Formen der Cybercrime, die von zum Teil hoher Arbeitsteilung geprägt sind (vgl. BAE-Detica, 2012; Broadhurst et al, 2013; Broadhurst et al, 2014; Chabinsky, 2010; Fortinet, 2013) und in denen nicht jede Geschäftsfunktion eine Funktion der Cybercrime im engeren Sinne darstellt. Organisierte Kriminalität (OK) im Bereich Cybercrime wurde unter Berücksichtigung dieser Aspekte in die Analyse mit aufgenommen (vgl. Kapitel 5.4 und 5.5). Das Thema wurde allerdings eher kurz abgehandelt, arbeitete das Bundeskriminalamt parallel zu dieser Erhebung doch in einem Forschungsprojekt mit, das sich auf EU-Ebene phänomenologischen Fragen von „Cyber-OK“ stellte.

Wie bereits das Beispiel der OK zeigt, sind Abgrenzungsschwierigkeiten auch Begrifflichkeiten geschuldet. Dies gilt beispielsweise für den Identitätsdiebstahl („identity theft“), einem Phänomen, das den Diebstahl bzw. die Erschleichung und den Gebrauch persönlicher Informationen (Morris, 2010) umfasst und insbesondere im angelsächsischen Raum diskutiert wird. Viele Arten der Gewinnung und Nutzung fremder Identitäten erfolgen allerdings in eher traditioneller Art und Weise zum Beispiel mittels Durchstöbern von Abfall nach persönlichen Informationen, das Nutzen öffentlich zugänglicher Quellen oder mittels Betrugshandlungen („identity theft“ als Teilmenge des „identity fraud“; vgl. Newman und McNally, 2005). In dieser Analyse findet der Identitätsdiebstahl lediglich Berücksichtigung, wenn ein Bezug zur Cybercrime im engeren Sinne deutlich erkennbar ist, bspw. in Form des Hackens von Computernetzen oder großer Datensammlungen (vgl. Kapitel 5.3.1).

3 Methodik

Das Wissen um Täter im Bereich Cybercrime ist begrenzt. Es basiert häufig auf retrospektiven Studien angeklagter Cybercrime-Fälle sowie Surveys und halbstandardisierten Befragungen (entweder Face-to-Face oder online) zu selbstberichteter Delinquenz. Eine zunehmend von Forschern genutzte Methode der Datensammlung besteht in der Beobachtung bzw. Analyse von Diskussionsforen (auch im „Darknet“) und Chat-Rooms (Broadhurst et al., 2013). Eine Auswertung von „Honeypots“ findet ebenfalls statt (Chiesa et al., 2009).

Soweit es um Surveys geht, die im Rahmen großer Hacker-Konferenzen mit zum Teil mehr als 10.000 Teilnehmern durchgeführt wurden, weist Dupont (2013) auf das Problem möglicher Verzerrungen in Richtung von „white-hat“-Hackern hin, die sich „unter die Mitarbeiter von Nachrichtendiensten und Polizei mischen“. In diesem Kontext sei darauf hingewiesen, dass die Identifizierung, Rekrutierung und das Interview von Kriminellen schon immer eine Reihe von praktischen und ethischen Dilemmata für Ethnographen mit sich gebracht hat, die auch in diesem Themenfeld eine Rolle spielen.

In zeitlicher Hinsicht berücksichtigt diese Erhebung öffentlich zugängliche Berichte, Aufsätze und Bücher seit dem Erscheinungsjahr 2000, die in deutscher oder englischer Sprache zum Themenkomplex vorlagen. Frühere Arbeiten wurden lediglich ausnahmsweise berücksichtigt, weil sie beispielsweise von grundlegender Bedeutung für das Thema oder auch für einzelne

kriminologische Erklärungen sind. Neben Ressourcenaspekten sprach für die genannte zeitliche Eingrenzung, dass es sich bei dem hier bearbeiteten Forschungsfeld noch um ein relativ junges handelt, das sich zugleich in einem Zustand permanenter Umwälzung befindet, der sich natürlich auch auf täterbezogene Phänotypen auswirkt.

Der Zugang zu den Medien erfolgte in erster Linie netzbasiert über das Internet, über Extrapol als Informations- und Kommunikationsplattform der deutschen Polizeien sowie über das Intranet des BKA. Im Internet wurden insbesondere die Suchmaschinen Google und Google-Scholar genutzt. Spezielle Suchbereiche umfassten Informationsangebote der Politik sowie von Wirtschaft und Verbänden (darunter u. a. Wirtschaftsprüfgesellschaften). In bibliothekarischer Hinsicht wurde in folgenden deutschsprachigen Angeboten recherchiert: COD-Literaturdatenbank (bundesweites Informationssystem für deutschsprachige polizeiliche Fachliteratur), Bibliothek der Deutschen Hochschule der Polizei, Bibliothek des Bundeskriminalamtes, Deutsche Nationalbibliothek, außeruniversitäre und universitäre (Forschungs-) Institute, GEPRIS (Geförderte Projekte Informationssystem der Deutschen Forschungsgemeinschaft) sowie TNS Emnid. Relevante englischsprachige Webangebote, auf denen gezielt nach Material gesucht wurde, betrafen das Home Office (UK), das National Institute of Justice – NIJ – (USA), die Royal Canadian Mounted Police – RCMP – (Kanada), Interpol, Europol sowie das Australian Institute of Criminology – AIC – (Australien).

In inhaltlicher Hinsicht wurde für die Recherche im Vorfeld zunächst eine deutschsprachige Liste relevanter Suchbegriffe mit Täterbezug erstellt. Im Detail waren dies Begriffe wie „Cybercrime“ / „Cyberkriminalität“ + „Täter“, „Cyber“ + „Täter“, „Internet“ + „Täter“, „Internetkriminalität“, „Computerkriminalität“, „Computer“ + „Täter“, „IuK“ + „Täter“, „Tätertypologie“, „Hack“ + „Täter“, „Hacker“, „Hacktivist“, „Täterprofil“ und „Tätertyp“. Parallel dazu nach den englischsprachigen Pendants gesucht, wobei „Täter“ übersetzt wurde als „offender“, „perpetrator“ und „criminal“. Darüber hinaus wurde nach feststehenden Begriffen wie „cracker“, „white hat“, „black hat“ oder „grey hat“ (zu den Begriffen vgl. Kapitel 5.1) gesucht. Die Recherchen wurden nachfolgend von zwei Mitarbeitern durchgeführt. Zu Literaturtreffern wurden Kurzzusammenfassungen erstellt, die wiederum für die Erstellung dieses Berichts genutzt wurden.

Die Arbeit hatte mit der Schwierigkeit zu kämpfen, dass es bislang kaum nach hohen wissenschaftlichen Standards durchgeführte kriminologische Untersuchungen zu Tätern im Bereich Cybercrime gibt. So basiert beispielsweise eine umfassende Erhebung des United Nations Office on Drugs and Crime zu Cybercrime (UNODC, 2013) in ihrem täterbezogenen Aspekt auf der systematischen Auswertung von lediglich vier Studien. McGuire und Dowling (2013a) verweisen in ihrem Review zu sog. „Cyber-dependent crimes“ für das Vereinigte Königreich (UK) ebenfalls auf einen Mangel an Evidenz.

Im Ergebnis ist damit nur wenig gesichertes Wissen zu den Themenfeldern Tätercharakteristika, Lebensläufe, Täterkarrieren, Verbindungen zwischen online- und offline-Taten, Weiterentwicklung in andere kriminelle Rollen sowie täterbezogene Prävention verfügbar (McGuire und Dowling, 2013a). In den Niederlanden werden genau diese Charakteristika in einer aktuellen Arbeit untersucht, zu der allerdings noch keine abschließenden Ergebnisse verfügbar sind (Kranenbarg, 2014).

4 Hackerphänomenologie

4.1 Begriff des „Hackers“ und kurzer geschichtlicher Abriss

Um die Frage zu beantworten, welche Typen von Hackern für die Gesellschaft besonders schädlich sind bzw. wie man sich ihrer erwehren kann, ist es notwendig, vorab den Begriff „Hacker“ als solchen zu erläutern. Diese Einführung erfolgt in stark geraffter Form und geht nicht detailliert auf alle Aspekte ein, existiert zwischenzeitlich doch eine „Myriade von Hacker-Definitionen“ (Holt und Kilger, 2012: 1). Eine umfassende und bei aller Kürze treffende Definition liefern Schell und Dodge (2002). Demnach sind Hacker Personen mit einem Interesse für Technologie, die ihr Wissen nutzen, um sich mit oder ohne Genehmigung Zugang zu Computern und anderen Geräten verschaffen.

Jordan und Taylor (2004) gehen einen Schritt zurück, in dem sie auf den Begriff „hack“ referenzieren, mit dem geschickte Programmiertricks umschrieben werden. Unter Hacks verstehen sie Versuche, Technologie in origineller, unorthodoxer und erfinderischer Art und Weise zu nutzen.

Ähnlich ist es in der freien Enzyklopädie Wikipedia formuliert: Demnach bezieht sich der Begriff in seiner ursprünglichen Verwendung „auf Tüftler im Kontext einer verspielten selbstbezüglichen Hingabe im Umgang mit Technik“. Es geht um „eine Art einfallsreiche Experimentierfreudigkeit mit einem besonderen Sinn für Kreativität und Originalität“, ohne dass Außenstehende einen Nutzen immer direkt erkennen können. Im Gegensatz zu der heute durchweg negativen Konnotation des Begriffes, für die exemplarisch die Definition von Taylor (1999) steht, der gemäß Hacking den unautorisierten Zugang und die nachfolgende Nutzung fremder Computersysteme darstellt, war der Begriff ursprünglich positiv besetzt (Kempa, 2006). Hacker ist insofern auch ein sozial konstruiertes Etikett, das sich über die Zeit durchaus verändert hat (Yar, 2005a).

Die ersten Versuche des Hackings gehen auf Studenten des Tech Model Railroad Club (TMRC) am Massachusetts Institute of Technology (MIT) ab dem Jahr 1955 zurück. In einer ursprünglich positiven Konnotation umschrieb der Begriff “hack” bei ihnen die Findung kreativer Lösungen bei technischen Problemen im Zusammenhang mit der Steuerung von Modelleisenbahnen (Krömer und Sen, 2011). Selber nannten sie sich „hacker“. Bereits die Anfänge des Hackings machen damit deutlich, dass Hacks nicht auf Computer beschränkt sein müssen, sondern technische Anlagen bzw. Technologiefelder jedweder Art umfassen können (Witte, 2013). Ein frühes und zugleich typisches Anwendungsbeispiel war das insbesondere ab den 70er Jahren in den USA verbreitete sog. „phreaking“, das die Manipulation von Telefonverbindungen bzw. das unerlaubte Einwirken auf Telefonvermittlungsstellen umschreibt, um umsonst Ferngespräche führen zu können (Hafner und Markoff, 1992; Kempa, 2006; Loper, 2009; Witte, 2013).

Hacking im Zusammenhang mit Computerprogrammierung trat am MIT erstmals Anfang der 60er Jahre auf und hatte seinen Bezug in der beginnenden Computerisierung der Universitäten. Damit ging eine akademische Hackerkultur (Wikipedia) einher, der es primär darum ging, die Leistungsfähigkeit der damals noch recht langsamen Großrechneranlagen durch geschickte Programmierung zu steigern. Ergebnisse sollten mit dem geringstmöglichen mathematischen Programmieraufwand erzielt werden (Krömer und Sen, 2011; Loper, 2009).

In den frühen 60er Jahren wurden auch erste Fälle des Hackings in der Form bekannt, dass

mit Computern derart Unwesen getrieben wurde, dass es zu finanziellen Schäden kam. „Hacking“ wurde zunehmend als kriminelles Handeln wahrgenommen was auf Seiten der ursprünglichen gesetzestreuen Hacker dazu führte, die anderen Hacker als „cracker“ zu etikettieren (Kempa, 2006). Unabhängig davon hat sich in der breiten Öffentlichkeit der Begriff „hacking“ als Synonym für die Gewinnung eines nicht autorisierten Zugangs zu fremden Computersystemen festgesetzt (Kirwan und Power, 2013).

Früh entwickelte sich auch eine eigene Hackerkultur, die davon getrieben war, Computertechnik als Chance zur Weltverbesserung zu begreifen. Bestrebungen und Reglementierungen bspw. im Zugang zu Computern, die dieser Vision im Wege standen, waren für Hacker nicht akzeptabel. Systeme sollten für jedermann zugänglich und zugleich veränderbar sein; der Zugang zum Computer sollte so frei und offen wie möglich gemacht werden (Levy, 1984). Statt Computern nur passiv zu begegnen, sollten ihre Möglichkeiten in kreativer Herangehensweise fortentwickelt werden. Der ungehinderte Zugang und Austausch von Informationen hatte in diesem Kontext besondere Bedeutung (Krömer und Sen, 2011).

Neben einer eigenen Hackersprache („hacker-jargon“) entwickelte sich eine Hacker-Ethik, nach der Zugang zu Computern beispielsweise grenzenlos und total sein, alle Information frei sein und Autoritäten misstraut werden sollte (Levy, 1984; Mizrach 1997[?]). Der Hackerjargon diente nicht allein dazu, ethische Vorstellungen und Werte von Hackern zu kommunizieren, sondern auch dazu, ihre sozialen Beziehungen untereinander zu strukturieren, ähnlich wie das in anderen Subkulturen der Fall ist (Holt, 2010). Das Bild des Hackers wurde u. a. durch das 1975 erstmals erstellte Hackerlexikon „The Jargon File“ geprägt, in dem über rein sprachliche Aspekte hinaus die Hackerkultur insgesamt eine Abbildung fand, die trotz aller Kritik das Bild des Hackers in der Öffentlichkeit mitprägte.

In neueren Arbeiten wird verstärkt darauf hingewiesen (u. a. Bissett und Shipton, 2000; Rogers, 2005; Kirwan und Power, 2013), dass das stereotype Bild des Hackers als das eines sozial eher inkompetenten jungen Mannes zwischen 14 und 18 Jahren, der bis in die frühen Morgenstunden an seinem Computer sitzt und sein technologisches Verständnis nutzt, gesichtslose und unmoralische Unternehmen zu attackieren, wenig realitätsnah ist. Hacker seien demnach eher durchschnittliche, unauffällige Personen mit allerdings teilweise herausragenden technischen Problemlösungsfertigkeiten, die wie andere auch am sozialen Leben mit Familie und Beruf partizipieren und dabei ihre Interessen ausleben (Chiesa et al., 2009; Pfeiffer und Telser, 2003). Was junge Hacker ebenfalls mit vielen anderen jungen Menschen gemein haben dürften, ist die von Chiesa et al. (2009) benannte Rebellion gegen alle Symbole oder Anzeichen von Autorität.

Viele Delikte der Cybercrime verlangen heute allerdings ein gewisses Maß an Organisation und Spezialisierung (UNODC, 2013). Damit hat sich das Bild von vorrangig isoliert agierenden Hackern überholt (Kaspersky und Interpol, 2014). Hinzu kommt die Möglichkeit, immer professionellere Dienstleistungen einkaufen zu können. „Cyber crime-as-a-service“ ist kein Einzelereignis mehr, sondern strukturelles Merkmal von Cyberkriminalität (Europol, 2015; NCSC, 2014). Auf dem Schwarzmarkt angebotene Dienstleistungen ermöglichen selbst weniger erfahrenen Kriminellen, ausgefeilte Cyberattacken auszuführen bzw. mit ihnen zu drohen (ebd.).

Die größte Bedrohung geht heute jedoch von professionellen Cyberkriminellen und staatlichen Akteuren aus (Geschonneck et al., 2015; NCSC, 2014). Letztere sind nicht allein bezogen auf den Aspekt der Cyberspionage von Relevanz, sondern verstärkt auch hinsichtlich der Möglichkeit zum Cyberwarfare, auf den viele Staaten verstärkt hinarbeiten (Gaycken, 2014).

4.2 Hackermerkmale

Die bereits vorgestellten Begriffsdefinitionen wie „hacker“, „cracker“ oder „phreaker“ deuten darauf hin, dass es *den* Hacker nicht gibt. Rogers (2005) hat dies mit dem Versuch verglichen, das gesamte Spektrum an traditionellen Straftätern (von Kaufhausdieben bis hin zu psychopathischen Mördern) in einer einzigen generischen Kategorie zusammenzufassen.

Bevor sich die Arbeit mit möglichen Klassifizierungen bzw. Typenbildungen bei Hackern befasst, erscheint es notwendig, mögliche Unterscheidungsmerkmale von Hackern weiter zu differenzieren. Neben biologischen und sozioökonomischen Merkmalen wie Alter, Geschlecht, Bildung, Beschäftigung/Einkommen, sind dies u. a. auch soziale und kommunikative Aspekte, Motivlagen und Angriffsziele.

4.2.1 Alter

Täter im Bereich Cybercrime sind auf der Basis der im Kapitel 3 bereits erwähnten systematischen Erhebung des UNODC (2013) in der Mehrzahl zwischen 18 und 30 Jahren alt. Im Einzelnen kommt die neueste der vom UNODC ausgewerteten Studien (BAE-Detica, 2012) zu dem Ergebnis, dass auch für die Zeit zwischen dem 30 und 40 Lebensjahr noch kriminelle Aktivitäten ausgewiesen werden. So waren 43% der Täter über 35 Jahre alt. Inwieweit das Thema dieser Studie, die Organisierte Kriminalität und ihre Arbeitsteilung, hier Auswirkungen auf das Ergebnis hat, dass 32 % der Täter zwischen 36 und 50 Jahren alt sind, lässt sich aus der Distanz kaum bewerten. Die bei UNODC (2013) eingeflossene HPP-Studie (Chiesa et al., 2009) weist ebenfalls darauf hin, dass sich das Durchschnittsalter der Hacker in den letzten Jahren dadurch erhöht, dass diejenigen, die fünf oder zehn Jahre zuvor begonnen haben, immer noch dabei sind.

Insgesamt ist allerdings von einer in hohem Maße jungen Hackerpopulation auszugehen, wie viele Studien zeigen (u. a. Allen et al., 2005; Dupont, 2013; Leukfeldt et al., 2013; Turgeman-Goldschmidt, 2011; Wilson et al., 2006; Woo 2003).

Lu et al. (2006) kamen auf der Basis der Auswertung von über 18.000 Cybercrime-Fällen des taiwanesischen Criminal Investigation Bureau für die Jahre 1999 bis 2004 auf einen Anteil von fast 30% in der Altersstufe der 18- bis 23-Jährigen. 45% der Täter hatten die gymnasiale Oberstufe („senior high school“) besucht und 24% waren eingeschriebene Studenten gewesen.

In einer von Rheinberg und Tramp (2006) durchgeführten online-Befragung besonders engagierter Computernutzer in Deutschland (n=271) lag der altersbezogene Mittelwert bei knapp 25 Jahren, wobei die Befragten im Mittel über eine knapp zehnjährige Computererfahrung verfügten.

In einer Analyse von 151 typischen Cybercrime-Fällen, die zwischen 1996 und 2008 in den USA angeklagt wurden, lag der Anteil der Täter, die 25 Jahre alt oder jünger waren, bei 40%,

derjenigen zwischen 26 und 35 Jahren bei 35% und der über 35-Jährigen bei 25% (Li, 2008).

In der Untersuchung von Chiesa et al. (2009) lag der Anteil 10- bis 20-Jährigen bei 31%, was als Reaktion auf den Internetboom und die Verfügbarkeit von Angriffsinstrumenten über das Internet gewertet wurde. Dies würde aus Sicht des UNODOC (2013) wiederum gut zur Hackerkategorie der sog. „script-kiddies“ passen. 30% der Stichprobe waren zwischen 21 und 25 Jahre und 19% bis 30 Jahre alt. Jeweils 7% waren zwischen 31 und 35 Jahre sowie zwischen 35 und 40 Jahre und lediglich jeweils 3% 41 bis 45 Jahre bzw. über 45 Jahre alt. Das Durchschnittsalter für Frauen lag bei 27 und das für Männer bei 25 Jahren. Zu der von Chiesa et al. (2009) gestellten Frage, wann mit dem Hacken begonnen wurde, nannten 61% der Befragten ein Alter zwischen 10 und 15 Jahren, während 32% 16 bis 20 Jahre nannten. 5% hatten ihre Hackingaktivitäten zwischen 21 und 25 Jahren, 2% zwischen 26 und 30 und nur 1% in einem Alter über 40 Jahren begonnen.

In einer kleinen niederländischen Fallstudie zum Thema Hacking (n=47), zu der Leukfeldt et al. (2013) berichten, lag das Alter der Verdächtigen zwischen zwölf und 65 Jahren. Die Altersverteilung wich signifikant von der Altersverteilung der niederländischen Bevölkerung über 12 Jahren, wie auch von den Strafverfolgungsdaten insgesamt, ab. In der Stichprobe kamen jeweils ca. 21% der Hacker aus der Gruppe der 12- bis 17-Jährigen sowie aus der Gruppe der 18- bis 24-Jährigen. 17% waren 25 bis 34 Jahre alt, 25% 35 bis 44 Jahre, 11% 45 bis 54 Jahre und 4% 55 bis 64 Jahre alt.

Die Erkenntnisse aus der Auswertung eines kleinen (n=17), im Bereich Botnetze wirkenden Hackernetzwerkes, gegen das die kanadische Polizei ermittelte, bestätigt die Erkenntnis zum Teil sehr junger Täter. Die meisten berichteten, schon sehr früh, zum Teil schon mit acht Jahren das Interesse am Hacken gefunden und schon in der frühen Jugend Erfahrungen mit Botnetzen gemacht zu haben (Dupont, 2013).

Bezogen auf Deutschland hat die Studie von Vick und Roters (2003) zum Account-Missbrauch im Internet Relevanz. In der Stichprobe von Tatverdächtigen (n=599) lag das Durchschnittsalter bei etwa 22 Jahren, wobei die Altersgruppe der 16- bis 21-Jährigen mit 66% am häufigsten vertreten war. Von den Tatverdächtigen lebten fast drei Viertel (72%) zum Zeitpunkt der Tatbegehung noch bei den Eltern.

Bezogen auf das Thema Hacktivismus, dem politisch-aktionistisch intendierten Hacken, existieren kaum Studien zum Alter der Täter. Wie Füllgraf (2015) berichtet, lässt sich aus verschiedenen Quellen folgern, dass die Mehrheit der Hacktivisten zwischen 16 und 30 Jahren ist. So waren von den zwischen 2010 und 2012 festgenommenen 211 Mitgliedern von Anonymous 31 unter 18 Jahre, 62 zwischen 18 und 28 Jahren und 10 älter als 28 Jahre. Zu den restlichen 120 Mitgliedern liegen keine Angaben zum Alter vor. Von den 37 Beschuldigten, die in einer Fallanalyse des Bundeskriminalamtes zum Hacktivismus jüngst genauer untersucht wurden, war auch hier, ähnlich zu der Altersverteilung der festgenommenen Anonymous-Mitglieder, die Mehrheit zwischen 14 und 28 Jahre alt; lediglich acht Beschuldigte waren über 28 Jahre alt (ebd.).

Nach Aussage von Krömer und Sen (2011) sind viele Mitglieder der organisierten Raubkopiererszene (Release- bzw. Warez-Szene) bereits über 30 alt. Vor dem Hintergrund eines boomenden Marktes legaler Video on Demand-Angebote, wie sie von Anbietern wie

Maxdome, Amazon oder auch Netflix kommen, stellt sich hier jedoch die Frage, welcher Raum bzw. wo zukünftig Raum für eine illegale Szene bleibt.

Vorliegende Erkenntnisse zum Lebensalter von Hackern und Virenschreibern deuten nicht zuletzt an, dass die meisten früh starten und im Alter von Anfang bis Ende Zwanzig bereits wieder aussteigen (Gordon, 2000; Yar, 2005a). Die Gründe für das „Herauswachsen" aus der Devianz könnte wie in anderen Feldern der Jugenddelinquenz in der Übernahme von Verantwortung liegen, die sich am Eingehen einer festen Beziehung, an der Gründung einer Familie oder auch in der beginnenden Berufstätigkeit – teils über den zeitlichen Umweg des Studiums – manifestiert. Computerkriminalität wäre insofern als typisches Beispiel für die adoleszente Krise zu interpretieren.

4.2.2 Geschlecht

Auch wenn die Situationsbeschreibung von Levy (1984), dass es noch nie einen weiblichen Hackerstar gegeben habe, in der Sache überholt sein dürfte, wie die Website „10 Notorious Female Hackers" (Computer Science Degree, 2013) belegt (vgl. auch Gyapjas, 2015), werden Cybercrime-Täter doch in der Mehrzahl als männlich (Allen et al., 2005; Holt et al., 2009; Li, 2008; Leukfeldt et al., 2013; Lu et al., 2006; UNODC, 2013; Steinmetz, 2015; Turgeman-Goldschmidt, 2011; Wilson et al., 2006; Woo, 2003) beschrieben.

Vick und Roters (2003) sowie Rheinberg und Tramp (2006) stützen diese Erkenntnisse für Deutschland mit einem Frauenanteil von lediglich 6% bzw. 13% in ihren jeweiligen Untersuchungen.

Die Szene organisierter Raubkopierer (Release- bzw. Warez-Szene) wird ebenfalls in der Mehrzahl als männlich beschrieben (Krömer und Sen, 2011).

In der zum Thema Hacktivismus durchgeführten Fallananlyse des BKA waren immerhin 24% der Täter weiblich, wobei die Stichprobe mit 37 Beschuldigten aus nur einem Verfahren relativ klein war und Füllgraf (2015) selber auf mögliche Selektionseffekte hinweist.

Chiesa et al. (2009: 90) sehen das Jahr 2001 als Wasserscheide zwischen einer Männer-dominierten Umgebung und einer, in der sich zunehmend auch Frauen finden. Gab es in der Dekade 1990 bis 2000 noch praktisch keine Hackerinnen, ist aus ihrer Sicht seitdem ein „exponentielles Wachstum" zu verzeichnen.

Auf der anderen Seite zeigt die Auswertung einer kleinen kanadischen Tätergruppe, die im Bereich Botnetze tätig war, dass junge Frauen lediglich als ehemalige, gegenwärtige oder potenzielle Freundinnen der männlichen Täter in Erscheinung traten, die entweder technische Hilfe benötigten oder aber zu Attacken anstifteten, niemals jedoch als Ersteller oder Betreiber von Botnetzen (Dupont, 2013).

4.2.3 Familiärer Hintergrund:

Viele der von Chiesa et al. (2009) befragten Hacker stammen aus benachteiligten bzw. problembelasteten oder dysfunktionellen Familien (alleinerziehend, Scheidung, Alkoholabhängigkeit, Adoptionen etc.). Einige haben zudem konfliktbeladene Beziehungen zu ihren Eltern. Hacking oder Phreaking werden als Möglichkeit beschrieben, diesem Leben

zu entfliehen und eine eigene Persönlichkeit zu entwickeln. Die Autoren geben allerdings keine Hinweise darauf, inwieweit die festgestellten familiären Probleme von denen anderer Jugendlicher bzw. Heranwachsender abweichen.

In der Untersuchung von Dupont (2013) kamen drei von 17 Hackern aus dysfunktionalen Familien, in denen ein oder beide Elternteile zum Teil auch wegen schwerer Delikte vorbestraft waren. Für diese Personen sieht der Autor das Hacken eher als die Ausweitung oder Diversifikation einer beginnenden kriminellen Karriere als einen Fehltritt in einer ansonsten ruhigen Biographie. An dieser Stelle ist allerdings anzumerken, dass in diesem Sample fünf Hacker auch über strafrechtliche Vorerfahrungen mit der Polizei berichteten.

4.2.4 Sozioökonomischer Hintergrund:

Die von Chiesa et al. (2009) befragten Hacker bildeten alle sozialen Schichten ab. Sie stammten sowohl aus benachteiligten Wohngebieten und waren der Unterschicht zuzuordnen als auch aus der Mittel- und Oberschicht. Häufig handelte es sich in diesem Sample um Kinder von Immigranten, die in verarmten suburbanen Gegenden (Vororte) wohnten.

Füllgraf (2015) berichtet, dass eine zum Thema Hacktivismus durchgeführte Literaturanalyse keine einschlägigen Untersuchungen zum sozioökonomischen Hintergrund von Hacktivisten zu Tage gefördert hat. So ist bislang nicht bekannt, aus welchem sozialen Umfeld Hacktivisten vornehmlich stammen.

4.2.5 Bildung

Woo (2003) berichtet von einer online-Befragung von Hackern (n=1.385), in der 3% angaben, in einem Ph.D.-Kurs zu sein (Graduiertenstudiengang). 5% der Befragten machten einen Master-Abschluss (Graduiertenstudiengang), 27% der Befragen befanden sich in einer vierjährigen Collegeausbildung, 14% in einer zweijährigen Collegeausbildung, 25% in der High School, 12% in der Mittelschule und 15% in der Grundschule.

In der Untersuchung von Chiesa et al. (2009) hatten 37% der Befragten die High School abgeschlossen, 25% verfügten über Ausbildungsnachweise, 10% hatten ein Aufbaustudium/Postgraduiertenstudium erfolgreich abgeschlossen und 7% eine standardmäßige Hochschulausbildung. 16% hatten einen Abschluss vergleichbar der deutschen Realschule und 4% vergleichbar der deutschen Grundschule. In der Befragung war es den Autoren auch darum gegangen, deutlich zu machen, dass Hacking keine Standardschulbildung erfordert. Zudem sollte gezeigt werden, so die Hypothese, dass die technischen Fertigkeiten von Hackern nicht an einen bestimmten schulischen Hintergrund bzw. an ein bestimmtes Schulniveau gekoppelt sind. Die Untersuchung hat ferner zu Tage befördert, dass Hacker insbesondere naturwissenschaftliche Fächer wie Physik, Chemie, Mathematik oder Computerwissenschaften gerne studieren bzw. studiert haben.

In einem Sample von 54 israelischen Hackern verfügten 74% über eine Bildungskarriere von 12 Jahren und mehr (Turgeman-Goldschmidt, 2011).

Holt et al. (2012) berichten, dass Hacker es wertschätzen, sich selber fortzubilden. Steinmetz (2015) berichtet in diesem Kontext, dass sich Hacker ihre Fertigkeiten weitestgehend alleine nach dem Prinzip von „trial and error“ in einem Selbstlernprozess aneignen.

Eine zum Thema Hacktivismus im Auftrag des BKA durchgeführte Literaturanalyse hat keine Erkenntnisse erbracht, über welchen Bildungsstand Hacktivisten verfügen. In einer vom BKA durchgeführten Fallanalyse sind allein die sozioökonomischen Merkmale Bildung und Beschäftigungsstatus erhoben worden, lieferte das Material darüber hinaus doch keine weiteren sozioökonomischen Merkmale. Zum Bildungsstand wurden in 27 von 37 Fällen überhaupt keine Angaben gemacht. Von den restlichen zehn Beschuldigten verfügten acht über einen Realschulabschluss, einer hatte das Abitur und einer besaß den Hauptschulabschluss. In Anbetracht der mangelnden Repräsentativität dieser Ergebnisse wäre es gewagt daraus zu schließen, dass die Mehrzahl hacktivistischer Taten von Angehörigen der mittleren Bildungsschicht begangen wird (Füllgraf, 2015).

4.2.6 Beschäftigung/Einkommen

Aussagen zur Beschäftigung und zum Einkommen liegen bislang kaum vor. In der von Chiesa et al. (2009) befragten Hackerstichprobe (n=547) hatten sich 8% der Oberschicht, 44% der oberen Mittelklasse, 37% der unteren Mittelklasse und 11% der Unterschicht zugeordnet.

In der von Turgeman-Goldschmidt (2011) untersuchten Stichprobe israelischer Hacker (n=54) lag das Einkommen zu 74% über dem Durchschnitt der Bevölkerung, was angesichts eines Bildungsstandes von durchweg mehr als zwölf Jahren nicht unbedingt überrascht.

Zum Beschäftigungsverhältnis einer Stichprobe von 37 Hacktivisten berichtet Füllgraf (2015), dass es sich bei 19 Beschuldigten um Schüler, Studenten oder Auszubildende handelte, was im Zusammenhang mit der Altersverteilung zu erwarten war. Vier Beschuldigte waren arbeitslos und einer angestellt. In 13 Fällen lagen Informationen zum Beschäftigungsverhältnis nicht vor.

4.2.7 Soziale Kontakte, Zusammenarbeit und Kommunikation

Kirwan (2006; aus Kirwan und Power, 2013) hat festgestellt, dass Hacker verglichen mit einer Kontrollgruppe von nicht hackenden Computernutzern über schwächere Beziehungen zu Familienmitgliedern berichteten. Zusätzlich zeigte die Kontrollgruppe höhere Werte auf einer Skala interpersonaler Beziehungen. Deutliche Unterscheidungen zwischen „white-hat“- und „black-hat“-Gruppen wurden allerdings nicht gefunden (zu den Begriffen vgl. Kapitel 5.1). Diese Ergebnisse wurden gestützt durch inhaltliche Auswertungen von Bulletin-Boards von Hackern, nach denen Hacker fähig sind, enge Beziehungen einzugehen, wobei sie allerdings diesbezüglich mehr Schwierigkeiten zu haben scheinen, als „normale“ Computernutzer.

Gegebenenfalls präventionsbezogen interessant ist die Frage, welche der sozialen Kontaktpersonen von den Hackingaktivitäten wussten. In der Untersuchung von Chiesa et al., (2009) waren lediglich ein knappes Drittel (32%) der Eltern informiert, während es unter den Freunden 27%, den Klassenkameraden 13 %, bei Partnern 11%, unter Kollegen 10%, bei den Lehrern 8% und bei den Arbeitgebern 7% waren.

Hacker sind „self-starter“ und streben nach Autonomie (Holt et al., 2012; Steinmetz, 2015).

Dennoch benötigen Hacker gerade am Anfang ihrer Karriere Mentoren, um die für das Hacken notwendigen Fertigkeiten zu erwerben. Später präferieren Hacker auch die Informationsgewinnung eher alleine durchzuführen, weil sie sich so sicherer fühlen und gleichzeitig die Entdeckungswahrscheinlichkeit verringern. Dennoch werden zum Teil temporäre Zusammenarbeitsformen gesucht, wenn es beispielsweise notwendig erscheint, auf spezifische Fertigkeiten zurückgreifen zu müssen, weil man diese nicht selber besitzt (Chiesa et al., 2009). Sobald mit anderen kooperiert wird, erfolgt die Arbeit sowohl online wie offline in kleineren losen sozialen Netzwerken. Kollegiale Beziehungen ermöglichen den Austausch an Informationen, Werkzeugen, normativen Werten und Zielen. Auf der Basis einer ethnografischen Untersuchung vergleicht Steinmetz (2015) die Gemeinschaft der Hacker als mit einer Handwerkszunft vergleichbar, in der eine Zusammenarbeit lediglich dann erfolgt, wenn sie notwendig ist.

Während in der weltweiten Untersuchung von Chiesa et al. (2009) 55% der Befragten angegeben haben, dass sie ausschließlich alleine arbeiten würden, gehörte die Mehrheit der als Hochrisikoakteur klassifizierten Hacker einer Untersuchung russischer Hacker zwei Gruppen an (Holt et al., 2012). Hier wurden diejenigen Personen, die mehreren Gruppen angehörten, als am gefährlichsten eingeschätzt, spielen sie u. a. doch auch eine besondere Rolle in der gruppenübergreifenden Kommunikation (ebd.).

Leukfeldt et al. (2013) berichten zu zwei niederländischen Untersuchungen, davon eine Fallstudie, nach denen Fälle von Hacking (n=54) zu 83% von Einzeltätern, zu 14% von zwei Tätern und zu lediglich 3% von drei und mehr Tätern begangen wurden. Die Fälle, in denen mehr als ein Täter handelte, bedeuten aus Sicht der Autoren nicht notwendigerweise, dass es sich um Bekannte oder um gemeinschaftlich agierende Täter handelte. Lediglich in knapp 5% der Hackingfälle waren Verdächtige Angehörige einer kriminellen Gruppierung, in der man sich kannte und zusammenarbeitete. Die in der Fallstudie ausgewerteten Taten sprechen aus Sicht der Autoren dafür, dass Hacking eine Straftat ist, die gewöhnlich außerhalb organisierter Gruppen begangen wird (ebd.).

Betrachtet man diejenigen Hacker, die zu mehr als einer Gruppe gehören, ist eine gewisse Volatilität der Gruppen feststellbar. Chiesa et al. (2009) berichten, dass es wohl häufiger passiere, dass Mitglieder austreten bzw. die Gruppen auflösen würden, um neue Gruppen zu gründen. Gerade für Jugendliche können diese Gruppen interessant sein, z. B. weil die Untergrund-Welt einen gewissen Reiz ausübt. Bei Jugendlichen dürfte zudem eine Rolle spielen, dass es für die Entwicklung einer Identität wichtig ist, sich zu Gemeinschaft zugehörig fühlen zu können. Die Gruppe hilft und unterstützt, bietet Zugehörigkeit und Schutz. Schließlich ist der größte Vorteil als Gruppe zu agieren, dass die Verantwortung geteilt ist und nicht nur bei einer Person liegt. Das bietet ein Gefühl der Sicherheit, wobei diese auch trügerisch sein kann, weil Fehler gemacht werden, die darauf zurückzuführen sind, dass die Wachsamkeit in der Gruppe nachlässt (Chiesa, et al., 2009).

Auch polizeilich interessant ist die Frage, ob Hacker Mitglieder ihrer Gruppe schon persönlich kennengelernt haben. In der Untersuchung von Chiesa et al., (2009) antworteten 37% der Befragten (n=182), dass sie alle Gruppenmitglieder persönlich schon einmal getroffen hätten. 34% gaben an, nur einen Teil der Gruppenmitglieder persönlich zu kennen, während weitere knappe 30% berichteten, noch nie eines der Gruppenmitglieder persönlich kennengelernt zu haben. Relevanz dürfte in diesem Kontext haben, dass 54% der Befragten

(n=180) angaben, dass sie weder in derselben Stadt noch im selben Land wie ihre Hacking-Partner leben würden. Im selben Land leben demnach 35% und in derselben Stadt wie ihre Hacking-Partner 11% (ebd.).

Zur Frage, wie Hacker miteinander kommunizieren, ist bekannt, dass Hacker bereits seit den späten 70ern bzw. Anfang der 80er Jahre die Möglichkeit der Mailbox zur Information und zum Wissensaustausch über Techniken des Hackings nutzen (Holt und Kilger, 2012; Holt, 2014). Später kam der Austausch über Internet Relay Chat (IRC)[2], Foren, Blogs, soziale Netzwerke und weitere online-Möglichkeiten hinzu. Im globalen Kontext kann die Art der Kommunikation untereinander dabei durchaus regionale Unterschiede aufweisen. So scheint es, dass russische Hacker-Gruppen IRC, Foren und bestimmte soziale Netzwerke wie Vkontakte oder LiveJournal und ICQ zum Instant Messaging sowie für den privaten Austausch nutzen während türkische Hacker den MSN-Messenger, Foren sowie E-Mail favorisieren. IRC scheint für sie eher weniger Wert zu haben. Chinesische Hacker wiederum scheinen auf Baidu und das Instant Messaging-Netzwerk QQ zu setzen. Die Kommunikation der Hacker ist dabei nicht allein auf die eigene Gruppe beschränkt, sondern umfasst z. T. die bereits genannten multiplen Mitgliedschaften (Holt et al., 2009; Holt et al., 2012; Holt und Kilger, 2012; Holt, 2014).

Die Untersuchungsergebnisse von Chiesa et al. (2009) lassen sich hingegen so deuten, dass der verschlüsselte Chat/IRC (66%) Normcharakter hat, gefolgt von geschlossenen privaten Mailing-Listen (7%). Der Anteil verschlüsselter E-Mails liegt mit 2% genauso niedrig wie der Anteil unverschlüsselter Mails. Dass auch noch alte Gebräuche gepflegt werden, zeigt der Anteil von 7% jeweils für unverschlüsselten Text-Chat/IRC und reale IRC-Treffen. Die Nutzung öffentlicher Mailing-Listen lag bei 1%.

Für den reinen Austausch von fachbezogenen Informationen nutzen Hacker ebenfalls mehrere Möglichkeiten. Gängige Praxis für kompetente Hacker ist beispielsweise der Gebrauch von Tutorials oder „how-to manuals“, um die Funktionsweise von Exploits zu erläutern (Holt und Kilger, 2012).

Über online-Kontakte hinaus berichten Hacker häufig auch über enge offline-Verbindungen zu Angehörigen der „realen Welt“, die ein Interesse am Hacking zeigen. Diese Verbindungen können bereits in der Schule entstehen und Netzwerken in anderen Bereichen ähneln. Eher hackertypisch sind offene Räume, sog. „hackerspaces“, in denen sich Hacker mit anderen Interessierten treffen. Berichtet wird von über 500 Hackerräumen weltweit, häufig in Lagerhallen oder großen Gebäuden, die von Non-Profit-Organisationen angemietet sind, um Interessierten die Möglichkeit zu geben, in einer offenen Umgebung mit neuen Technologien zu experimentieren. Diesen Hackerräumen kommt u. a. eine Mentorenfunktion zu, können am Thema Interessierte dort doch Hilfe und Unterstützung von fachkundigen Hackern bekommen. Kontakte zu Gleichgesinnten werden auch auf Hackerkonferenzen wie der „2600“ oder der seit 1993 stattfindenden „DefCon“ geformt. Diese Konferenzen haben darüber hinaus eine wichtige Funktion, wenn es darum geht, Konflikte in der Hacker-Community zu lösen, indem vor allem im Gegensatz zur online-Kommunikation der mündliche Diskurs und ebenso non-verbale Hinweise möglich sind (Holt und Kilger, 2012; Holt, 2014).

[2] Internet Relay Chat ist ein rein textbasiertes Chat-System, das Gesprächsrunden mit einer beliebigen Anzahl von Teilnehmern in so genannten Channels (Gesprächskanälen) ermöglicht.

4.2.8 Weitere Persönlichkeitsmerkmale

Dass die Beschreibung einer Hackerpersönlichkeit von erheblicher Komplexität ist, dürften die bisherigen Aussagen bereits angedeutet haben. Die Frage ist, ob eine derartige Aufgabe überhaupt sinnvoll ist, scheinen sich Hacker doch im Kern nicht von dem Rest der Bevölkerung zu unterscheiden.

Jordan und Taylor (1998), die als eine der ersten die Motivationen von Hackern untersucht haben, lehnen jeden Versuch ab, Hacker als pathologisch zu bezeichnen. Sie erklären die Hacking-Community bzw. die kollektive Identität von Hackern stattdessen mittels der Faktoren Technologie, Geheimhaltung, Anonymität, Personalfluktuation, männliche Dominanz und Motivation.

Woo (2003) hat in einer Befragung von Hackern die Verbindung von psychologischen Variablen und Hackingaktivitäten untersucht. Im Ergebnis berichteten stark narzisstische Hacker mehr Aggressivität als wenig narzisstische Hacker. Intrinsische wie extrinsische Motivation wies teilweise Bezüge zur Aggressivität auf. So zeigten stark nationalistische Hacker höhere Level im Bereich Aggressivität als wenig nationalistische Hacker. Die Untersuchung zeigt zudem, dass Hacker mit einem hohen Flow-Niveau tendenziell mehr in Hackingaktivitäten involviert waren als die mit einem niedrigen Flow-Level (zum Flow-Begriff vgl. Kapitel 6.7).

Unter Bezugnahme auf eine qualitative Untersuchung des emeritierten Professors für Soziologie an der Universität von Pittsburgh Lieberman schreiben Fötinger und Ziegler (2004), dass sich Hacker kaum vom „Normalbürger“ unterscheiden lassen - mit dem einzigen Unterschied, dass sie regelmäßig Straftaten begehen, indem sie sich in die Computer anderer Leute hacken. Sie sind demnach weder seltsam („weird“) wie in dem Film „Hackers“ noch sind sie zerstörerisch wie in dem Film „War Games“. Auch für Hacker ist die Privatsphäre grundsätzlich wichtig, selbst wenn sie die anderer Leute in ihrem eigenen Handeln missachten. Hacker haben nach Lieberman auch keine Schwierigkeiten im Umgang mit anderen Menschen; die Aussage „unfähig zu normalen sozialen Interaktionen“ zu sein, trifft ebenfalls nicht zu.

Chiesa et al. (2009) hatten im Rahmen ihrer Befragung herauszufinden versucht, ob Hacker eher schüchtern oder selbstsicher, naiv oder gewieft, kontaktfreudig oder einzelgängerisch sind. Im offline-Leben ist ein Teil der Befragten wohl eher schüchtern, so die Erkenntnisse, während sie in ihrem „natürlichen Element“, der Cyberwelt, eine völlig andere Persönlichkeit offenbarten. Viele befragte Hacker kommunizieren sehr leicht auf elektronische Weise mit anderen, während diese Ungezwungenheit im richtigen Leben fehlt. Die Autoren erklären dies damit, dass das elektronische Medium als Barriere wirkt, die den Menschen versteckt und auch schützt. Die Autoren relativieren ihre Aussagen allerdings insoweit, dass die festgestellten Verhaltensunterschiede im Netz und in der realen Welt nicht nur für Hacker, sondern auch für andere Heranwachsende gelten.

Chiesa et al. (2009) haben im Rahmen ihrer Untersuchung auch erhoben, ob und inwiefern Hacking die psychophysische Seite ihrer Anwender beeinflusst. Relevanz hatten in dem Kontext die Anzahl der von Hackern genutzten Spitznamen und eine diesbezügliche mögliche

Verbindung zu Persönlichkeitsspaltungen, Alkohol- und Drogenabhängigkeiten auch in Bezug zur Trennung der Eltern von Hackern sowie psychophysische Probleme, die durch Hacken selber ausgelöst werden.

56% der Befragten gaben an, mehr als einen Spitznamen zu nutzen, während 44% nur einen Spitznamen verwenden (n=236). Der offenen Frage, ob im Falle der Verwendung von mehr als einem „nickname" die Befragten (n=103) *auch* das Gefühl hätten, über mehr als eine Persönlichkeit zu verfügen, stimmten 65% zu, während 35% die Frage verneinten, was die Autoren zugleich als Validierung der Gleichung „doppelter Spitzname = doppelte Persönlichkeit" interpretieren. Sie weisen allerdings zugleich darauf hin, dass Hacker in ihrem online-Handeln immer mindestens eine weitere Persönlichkeit übernehmen, ob nun für Hacking-Zwecke ein zweiter Spitzname verwendet wird oder nicht (ebd.).

Auf die Frage nach Subtanzmissbrauch (Alkohol und/oder Drogen) erklärten knapp die Hälfte (47%) der Befragten (n=543) in der Untersuchung von Chiesa et al. (2009), keinen Alkohol bzw. Drogen zu konsumieren, während jeweils 22% exzessives Trinken bzw. den Drogenkonsum und 10% den Konsum von Alkohol und Drogen angaben.

Bei insgesamt 129 auswertbaren Fragebögen zum Thema Trennung der Eltern kann der Alkohol- und Drogengenuss in 47% der Fälle korreliert werden mit der Zugehörigkeit zu einer Familie, in der die Eltern geschieden sind und die Familie in einer Großstadt lebt. 38% der Befragten haben Alkohol, getrennte Eltern und das Leben in der Großstadt gemeinsam. Nur 9% der Hacker mit getrennten Eltern, die aus kleinen Städten kommen, sind Drogennutzer und 6% alkoholabhängig (ebd.).

34% der Befragten (n=276) litten unter Schlaflosigkeit oder haben schon einmal darunter gelitten. Bei Angstzuständen waren das 27%. 20% gaben an, schon unter Paranoia gelitten zu haben, während 13% schon einmal Panikattacken hatten (ebd.).

34% der unter Schlaflosigkeit leidenden Befragten gaben an, dass die Ursache dafür das Hacken sei, während der Anteil bei Paranoia 28%, bei Angstzuständen 18%, für Halluzinationen 10% und für Panikattacken ebenfalls 10% beträgt (ebd.).

Bachmann (2010) hat untersucht, inwieweit die Hackern zugeschriebenen Persönlichkeitsmerkmale einer starken Präferenz für rationale Entscheidungen und einer ausgeprägten Neigung zu Risikoverhalten tatsächlich Hackingaktivitäten beeinflussen und welchen Einfluss sie auf den Erfolg haben. Beide Faktoren haben sich demnach als wertvolle Prädiktoren für den selbstberichteten Hackingerfolg erwiesen. Hacker mit einer stärkeren Präferenz für rationale Entscheidungsfindungsprozesse berichteten über eine größere Erfolgsquote als diejenigen Hacker, bei denen diese Eigenschaft weniger ausgeprägt war. Sie sind zudem an signifikant mehr Hackingversuchen beteiligt. Es scheint, dass sie sich sicherer fühlen, Ziele erfolgreich zu attackieren. Sie wenden durchdachtere Angriffsroutinen an, die wiederum zu besseren Erfolgen führen. Hacker mit einer weniger ausgeprägten Präferenz für rationales Denken scheinen über weniger Vertrauen hinsichtlich ihrer Fähigkeit zu verfügen, Angriffsziele erfolgreich zu attackieren, so dass sie auch weniger Angriffsversuche berichteten. Eine ausgeprägte Neigung zu Risikoverhalten ist ebenfalls signifikant hinsichtlich des Hackingerfolges sowie insgesamt bezüglich der Beteiligung an Hackingaktivitäten. Personen mit einer ausgesprochenen Risikonähe beteiligen sich demnach an mehr Hackingversuchen, berichteten insgesamt allerdings weniger Erfolge.

4.2.9 Motive

Turgeman-Goldschmidt (2011) zeigt mit den Ergebnissen seiner Befragung von 54 israelischen Hackern, dass unabhängig von Zahl und Schwere der begangenen Computerstraftaten , sowohl „gute“ als auch „schlechte“ Hacker ihr Handeln eher als das Überwinden von Grenzen („breaking boundaries“) bezeichneten bzw. als das Brechen von Konventionen („shattering conventions“) oder als das Unmögliche tun („doing the impossible“). Bekannt ist, dass sie sich eher als Abenteurer denn als Kriminelle sehen (Jordan und Taylor, 1998, 2004; Taylor, 1999).

Welche Motive darüber hinaus im Einzelnen Hacking beeinflussen können, soll nachfolgend herausgearbeitet werden. In der Literatur findet sich zu dem Thema eine Vielzahl von Arbeiten. Holt und Kilger (2012), die unter Bezugnahme auf Kilger, Stutzman und Arkin (2004) sechs Hauptmotivlagen der Hacker-Community beschreiben (Entertainment, Ego, Status, Zugang zu einer sozialen Gruppe, Geld und Ursache-basiert) weisen darauf hin, dass häufig keine Einzelmotive sondern Motivbündel Ursache des Hackings sind und Zuordnungen bzw. enge Abgrenzungen teilweise schwierig sind.

Für eine inhomogene Motivlage bzw. Motivbündel zum Teil mit Rechtfertigungsaspekten, die eigentlich handlungsleitende Motive überlagern, sprechen auch polizeiliche Daten (Picko und Hahn, 2007).

Herbst (2013) und Füllgraf (2015) haben jüngst die Motive von Hacktivisten untersucht. Da es sich beim Hacktivismus inhaltlich um die Schnittmenge der Konzepte Hacking und Aktivismus handelt, finden sich auch bei Hacktivisten Motivbündel, die in Teilen die aktivistische Seite und in Teilen die Hackerseite der Täter reflektieren. Hauptmotive sind Propaganda und Protest. Jedoch spielen auch der Spaßfaktor, die Verhinderung von Wettbewerb und von politischen Maßnahmen (wie z. B. Aussagen, Informationen im digitalen Bereich) im Wahlkampf sowie die wirtschaftliche und/oder politische Schwächung von Adressaten eine Rolle.

Nachfolgend werden häufig in der internationalen Literatur genannte Motivationen erläutert. Hinsichtlich der gewählten Differenzierung (vgl. nachfolgende Aufzählungspunkte) sei einführend angemerkt, dass diese nicht im Sinne abschließender, trennscharfer Kategorien zu verstehen ist. Ausgangspunkt für die Differenzierung war die ausgewertete Primärliteratur mit teilweise recht oberflächlichen Motivbeschreibungen.

- Spaß am Hacken, Unterhaltung („entertainment“), Neugier

Himanen (2001; aus: Rennie und Shore, 2007) hat auf die intrinsische Motivation und diesbezüglich auf den Unterhaltungswert hingewiesen, den das Hacken von Computernetzwerken mit sich bringt. Dieser stammt zumindest in Teilen von der Neugier und intellektueller Herausforderung, auszuprobieren, wie sich Passworte umgehen bzw. raten lassen und man Zugang zu fremden Computersystemen bekommt (s. a. Chiesa et al., 2009; Kirwan und Power, 2012; McGuire und Dowling, 2013a; Vick und Roters, 2003). Dieses Motiv korreliert mit der Wissbegier, dem nach Chiesa et al. (2009) von Hackern in der Selbsteinschätzung am häufigsten genannten Charakterzug.

Unterhaltung ist für Holt und Kilger (2012) ein seit den Anfängen des Hackings konstantes Motiv. Das intensive Verlangen, Technologie zu verstehen, bedeutet auch, mit dieser zu spielen bzw. sich mit der Beschäftigung mit ihr zu unterhalten und Spaß zu haben. Das wird nicht nur auf Hackerkonferenzen und Wettbewerben unter Hackern deutlich; selbst maliziöse Hacks können unterhaltenden Wert haben, wie Holt et al. (2008) berichten. Beispiel dafür ist auch das Konzept „lulz“ als Variation von „LOL“ oder „Laugh out loud“, das sich auch im Namen der Hackergruppierung „LulzSec“ befindet. Hauptziel dieser Gruppe war tatsächlich der Spaß am Hacken und die dadurch entstandene Schadenfreude (Füllgraf, 2015).

- Nervenkitzel („thrill“)

Eng mit den Aspekten von Neugier und spannender Freizeitunterhaltung ist im Gegensatz zur Langeweile des offline-Lebens der Nervenkitzel verbunden, der dadurch entsteht, dass Verbotenes ausprobiert wird – möglichst ohne dabei gefasst zu werden (Denning, 1999 [aus Woo, 2003]; Schneier, 2003). Chiesa et al. (2009) führen hier den Vergleich mit den Panzerknackern aus den Disney-Comics an: Je schwieriger Alarmsysteme seien, desto mehr würden sich die „Panzerknacker“ angestachelt fühlen diese zu überwinden - nur dass sie im Gegensatz zu den Disneyfiguren weniger gefasst würden. Loper (2009: 17) zitiert in diesem Kontext Aussagen überführter Hacker wie „*[H]acking is like cocaine… it’s a rush you can’t forget*“ oder „*Hacking is the next best thing to sex*“.

- Zugehörigkeit zu einer Gruppe

Hackerfertigkeiten bereiten die Grundlage, um Zugang zu Gruppen zu bekommen. Während gute Leistungen im Hacken in den 1980er und 1990er Jahren dazu führten, Einladungen für geschlossene Nutzergruppen zu bekommen, hat die einsetzende Spezialisierung im IT-Bereich dazu geführt, dass es heutzutage zunehmend schwierig für Hacker ist, alle Facetten neuer Technologien zu verstehen. In einer zunehmend arbeitsteiligen Welt des Hackens ist es für Hacker daher bedeutsam, Zugang zu Gruppen mit dem für sie relevanten Wissen zu bekommen (Holt und Kilger, 2012).

Das Streben nach Zugehörigkeit zu einer Gruppe ist ein weiterer Motivaspekt, der gerade für jugendliche Hacker Relevanz hat (Chiesa et al., 2009). Das gilt dabei nicht allein für diejenigen, denen das Eingehen von Beziehungen zu realen Menschen zu herausfordernd bzw. komplex ist (Rennie und Shore, 2007). Motiv scheint auch zu sein, wertvolle Informationen innerhalb der eigenen Community zu steuern, zum Teil auch, um abhängig von ideologischen, thematischen oder sonstigen Gründen gegen anderen Hackergruppen vorgehen zu können (Woo, 2003).

- Ruhm, Status, Glorifizierung

Zu dem gruppenbezogenen Motivationsaspekt gehört letztlich auch das Streben, von anderen respektiert und bewundert, ggf. sogar berühmt zu werden. So werden fremde Webseiten zum Teil verändert (sog. Web-Defacements), um Freunden zu imponieren (Woo, 2003). Da die Hackergemeinschaft zugleich eine Leistungsgesellschaft (Meritokratie) ist, in der Individuen nach ihren Fähigkeiten und Fertigkeiten bewertet werden, bieten anerkennungswürdige Leistungen die Möglichkeit, in der Hierarchie der eigenen Hackercommunity aufzusteigen, wie Hackerlegenden wie Kevin Mitnick belegen (Chiesa et al., 2009; Hold et al., 2012; Holt und Kilger, 2012; Kempa, 2006; Kirwan und Power, 2012; McGuire und Dowling, 2013a).

In der organisierten Raubkopiererszene (Release- bzw. Warez-Szene) geht es den handelnden Akteuren in erster Linie um die Gewinnung von Status und Ruhm und nicht von finanziellem Profit. Für Jeff Howe ist daher ultimatives Ziel „*Beat the street date of a big-name album, videogame or movie by as much time as possible.“* (Howe, 2005; zitiert in Krömer und Sen, 2011: 49)

Als Verstärker von Ruhm und Glorifizierung wird die Medienlandschaft mit ihrer Sensationsgier und zugleich Verurteilung von Hackingattacken genannt. Die Industrie sendet ebenso verwirrende Botschaften, in dem bspw. Hackerchallenges organisiert und ehemalige Hacker als Sicherheitsberater angeheuert werden (Rennie und Shore, 2007).

- Macht und Kontrolle

Der Erwerb von Macht und Kontrolle über Computersysteme eines Staates, von Banken oder anderer Institutionen werden ebenfalls als Motiv genannt (Chiesa et al., 2009; Grabosky, 2000; Füllgraf, 2015). Große intellektuelle Herausforderungen können dabei mit Allmachtsgefühlen einhergehen (Kempa, 2006). Nach Rist (1998) ist ein primärer Motivationsfaktor für das Hacking eine Mischung von Ego und politischer Kommentierung, was sich in Denkarten „Ich bin schlauer als Du; check mal Deine Website“ äußert (zitiert in Woo, 2003: 13). Egoaspekte stehen für Holt und Kilger (2012) jedoch in permanentem Widerspruch zu Aspekten der Geheimhaltung, birgt die Offenbarung von in der Community hochangesehenen innovativen Verfahren doch immer das Risiko, auch Strafverfolgungsbehörden auf den Plan zu rufen.

- Monetäre bzw. wirtschaftliche Gründe

Monetäre Motive in Bezug auf Hacking sind eher neuerer Natur, was mit der zunehmenden technologischen Durchdringung vieler gesellschaftlicher Bereiche zu tun hat. Während Geld als Motiv in den 80ern deshalb eine eher geringe Rolle spielte, weil digitale Güter im normalen Alltag erst wenig existierten, hat die Abhängigkeit von technologischen Ressourcen im öffentlichen und privaten Sektor zu einer stark veränderten Situation geführt. Als Ergebnis richten sich Hackerangriffe heute häufig an Institutionen in den Bereichen Einzelhandel und Finanzen. Illegal erlangte Daten können dabei zunehmend über offene Märkte in Profit umgesetzt werden (Holt und Kilger, 2012). Rennie und Shore (2007) verweisen diesbezüglich auf die geldwerten Belohnungen, die der Diebstahl von Kreditkartennummern, das Verändern von Dokumentationen oder das Stehlen von Identitäten mit sich bringen kann.

Weitere Facetten wirtschaftlicher Motivationen finden sich bei Hackern, die ihre Programme im Dark Net verkaufen oder bei „Berufshackern“, die ihr Können Unternehmen oder auch dem Staat zur Verfügung stellen (Kempa, 2006).

- Politische Gründe (im weitesten Sinne)

Holt und Kilger (2012) stellen über die letzten zwei Dekaden eine Zunahme von Hacking-Angriffen fest, die ihre Ursache in politischen, nationalistischen und religiösen Anschauungen haben. Diese Form der Angriffe hängen stark davon ab, wo Hackergruppierungen regional in der Welt verortet sind und welche kulturellen, ideologischen, politischen oder religiösen Orientierungen ihr Handeln steuern. Beispiel sind hacktivistische Angriffe von Anonymous gegenüber MasterCard, Visa und PayPal, nachdem diese Institutionen finanzielle Dienstleistungen für WikiLeaks beendet hatten (Füllgraf, 2015; Herbst, 2013). In einer Studie von Woo et al. (2003) betrafen 20% der Stichprobe einer Inhaltsanalyse politisch motivierte Web-Defacements. Während hacktivistische Täter bzw. Gruppen es bei aktivistischen, gewaltfreien Taten belassen, geht es Cyberterroristen darum, mit Methoden des Hackings bzw. der Zerstörung von Informations- und Kommunikationstechnologie politische Entscheidungsträger zu beeinflussen, die Bevölkerung zu verängstigen und letztlich politische Verhältnisse in ihrem Sinne zu verändern (NCSC, 2014).

Weitere politische Themen betreffen die Bekämpfung von Kinderpornographie oder jihadistischer Gewalt (Foster, 2015; Füllgraf, 2015; Herbst, 2013; Woo, 2003). Einer der Katalysatoren für Hacking scheint zudem der Nationalismus zu sein (Woo, 2003).

Kempa (2006) versteht unter politischen Gründen letztlich auch den Aspekt des sich Wehrens vor der eigenen Kriminalisierung als Hacker. Abgeleitet aus der Hackerkultur geht es um die Akzeptanz einer im weitesten Sinne kritisch-kreativen Computernutzung nach dem normativen Ideal des Jargon File.

- Schadensabsicht und Rache

Die Herbeiführung eines Schadens muss nicht absichtlich erfolgen (Gnörlich, 2011). In der Untersuchung von Chiesa et al. (2009) haben lediglich 20% der Hackerstichprobe (n=219) die Frage bejaht, ob sie davon ausgehen, mit dem Hacken andere geschädigt zu haben.

Beim Thema Schadensabsicht dürften politische Motivlagen eine ganz besondere Rolle spielen, geht es auch hier doch häufig um das Ziel der Schädigung oder Bestrafung (Füllgraf 2015; Herbst, 2013). Wie bereits ausgeführt, ist das Ziel der Schadensherbeiführung dem Cyberterrorismus immanent. Eine besondere Relevanz dürfte der Wille zur Schädigung auch bei den sog. „Innentätern“ haben (IBM, 2015).

- Sucht

Sucht bzw. die Computerabhängigkeit, aber auch der Zwang zu hacken, werden als Motivlage im Zusammenhang mit dem Streben nach dem wiederkehrenden „Kick“ oder „Thrill“ genannt, der entsteht, wenn etwas Verbotenes getan wird (Kempa, 2006). Bekanntheit hat die „Suchtanalogie“ u. a. im Zusammenhang mit der Hackerlegende Kevin Mitnick erlangt, der 1989 zu einer Suchttherapie verurteilt worden war (Loper, 2009). Yar (2005a) spricht in diesem Kontext von der „Medikalisierung“ des Hackens als einer psychologischen Erkrankung („Internet Addiction Disorder“), die im deutschsprachigen Raum als Internet- bzw. Onlinesucht diskutiert wird. Eine in Deutschland 2010 durchgeführte repräsentative Studie zur Prävalenz der Internetabhängigkeit (Rumpf et al., 2011) gibt allerdings keine

unmittelbaren Hinweise auf eine Verbindung von Internetabhängigkeit und Hacking.

Aus Sicht von Chiesa et al. (2009) scheint eine wie auch immer geartete Abhängigkeit vom Hacken zwar nicht die Masse an Hackern zu betreffen, aber doch Relevanz zu haben, wie ihre Erkenntnisse aus dem HPP zeigen. 47% (n=225) der von ihnen befragten Hacker hatten angegeben, nie Entzugserscheinungen gespürt zu haben, während 40% diese selten oder wenig („rarely“) zeigten. 14% haben demnach immer Entzugserscheinungen gehabt.

Den Bereich „Sucht“ verlassend sei nachfolgend ihrer offenen Herangehensweise wegen die Arbeit von Rheinberg und Tramp (2006) besonders erwähnt. Diese haben in einer online-Befragung von 271 besonders engagierten Computernutzern in Deutschland, die über besondere Verteiler (z. B. relevante Fachschaften, Chaos Computer Club) gewonnen wurden, deren Anreiz- bzw. Motivspektrum erhoben. Rheinberg und Tramp (2006) haben nachfolgend auf der Basis von Selbstauskünften ihrer Stichprobe fünf Nutzungstypen gebildet (Unterhaltungssuche, zweckorientierte Nutzung, Hacking, Cracking und Hardware-Basteln).

Nachfolgend werden die in der Untersuchung gebildeten Skalen in der Reihenfolge ihrer Gewichtung präsentiert:

(1) Zugehörigkeit/Gemeinschaftsgefühl

Hier ging es um soziale Aspekte der Computernutzung („weil meine Freunde auch programmieren“, „um in einer Gruppe komplexere Systeme zu bearbeiten“).

(2) Kompetenzerleben bzw. Kompetenzerweiterung

Hier wird besonders geschätzt, dass man am Computer selbstbestimmt seine Anforderungen wählt („weil ich mir meine Herausforderungen selber aussuchen kann“) und den Zuwachs eigener Kompetenzen sehen kann („weil ich am Ergebnis sehen kann, dass ich immer besser werde“).

(3) Vielseitigkeit und Nutzen

Hier werden die Aspekte der Interaktion mit Computern thematisiert, die typischerweise als Gründe vermutet werden, warum man sich in seiner Freizeit vor den „Bildschirm einer Rechenmaschine setzt, statt etwas viel Schöneres zu tun“.

(4) Vermeidung von Langeweile

Hier geht es um den Aspekt, dass man mangels Alternativen vor dem Computer sitzt („weil ich sonst nichts anderes zu tun habe“)

(5) Rebellische Illegalitätstendenz/Sensation Seeking/Prestigesuche

Diese hochreliable Skala wies zwar für die Gesamtstichprobe den geringsten Anreiz aus, hatte allerdings für den Typ des Crackers das höchste Anreizgewicht.

Insgesamt liegen die motivationalen Gewichte aus Sicht von Rheinberg und Tramp (2006) überraschenderweise bei den sozialen Aspekten der Tätigkeit, gefolgt von der reinen Leistungsthematik. Die Vielseitigkeit des Einsatzes von Computern spielte in dieser Stichprobe besonders engagierter Computernutzer keine besondere Rolle und die Vermeidung von Langeweile ebenfalls nicht. „Rebellische Zerstörungsfreuden“ und/oder das Streben nach Anerkennung und Prestige waren allenfalls für Untergruppen interessante Anreize.

Abschließend sei in aller Kürze auf einige grundlegenden Kritiken zum Thema Motivationen verwiesen. So beschreibt Yar (2005a) die Situation derart, dass von Strafverfolgungsbehörden vorgenommene Fremdzuschreibungen tendenziell eher das Boshafte und Schlechte in der Motivation betonen, während in der öffentlichen Diskussion ein weiteres Bündel an Motiven wie Durchsetzungskraft, Neugier und die Suche nach Nervenkitzel, Gier und Hooliganismus eine Rolle spielen. Gerade die letztgenannten Aspekte referenzieren allerdings auf bekannte soziale Konstrukte der Jugenddelinquenz. Sofern man Hacker selber nach ihren Motiven befragt, werden regelmäßig Motive genannt, die der Hackerethik einer früheren Generation von Computerenthusiasten entsprechen (Yar, 2005a). Auf das Problem, bei der Befragung von Hackern deren *ex ante*- Motivationen von *ex post*-Rechtfertigungen zu unterscheiden, weist Taylor (1999) explizit hin.

Im Hinblick auf Typisierungen von Hackern sei zudem daran erinnert, dass sowohl Hacker mit Schädigungsabsicht als auch solche ohne diese Absicht zumindest einen Teil der Motivlagen teilen können. Bei den genannten „white hats“ und „black-hats“ liegt beispielsweise das gruppenspezifische Unterscheidungsmerkmal in der Art der Wirkung, die erzielt wird (gutartig bzw. Schäden vermeidend vs. bösartig bzw. Schäden herbeiführend).

4.2.10 Fertigkeitsniveau

In der Erhebung von Chiesa et al. (2009) wurde gefragt, wie Hacker ihr Fertigkeitsniveau selber einschätzen. Lediglich 22% der Befragten (n=273) sahen sich selber als Experte. Gleich viele antworteten, dass sie über hohe technische Fertigkeiten verfügen. 35% sahen demgegenüber ihr Niveau als durchschnittlich an, während 21% ihr Können sogar als niedrig einstuften.

Dupont (2013) berichtet aus seiner Untersuchung eines Hackernetzwerks, gegen das die kanadische Polizei ermittelt hatte. Auf der Basis einer von Copes und Vieraitis (2008) für Identitätsdiebe entwickelten Typologie beschreibt er drei Arten von Fertigkeiten, über die Hacker, die auch wirtschaftlich bestehen wollen, verfügen sollten: (1) technische (Welche technischen Voraussetzungen erfordert bspw. ein stabiles Botnetz?), (2) monetarisierungsbezogene (Wie arbeiten Finanzinstitute? Welche Identifikationen sind notwendig?) und (3) soziale (Fähigkeit, die soziale Situation durch verbale und non-verbale Kommunikation zu manipulieren).
In technischer Hinsicht war nur einer von zehn Hackern der Gruppierung in der Lage, den Malware-Code für seit Jahren am Markt verfügbare Botnetze (dBots und Varianten) zu verändern. Er wirkte als Mentor und Lehrer für die anderen Gruppenmitglieder und betrieb das größte Botnetz mit 291.000 Bots. Das technische Können der anderen Hacker war eher bescheiden. Beispielhaft für die geringe technische Expertise steht ein Täter, der zwar 104.000 Bots kontrollierte, allerdings lediglich neun Kreditkartendaten erlangt hatte. Für diese Hacker war es zudem schwer, die notwendige Infrastruktur zu unterhalten, wenn ihre Bots und C&C-Server, die alle auf kompromittierten Maschinen liefen, entdeckt und entfernt worden waren. Diese uneinheitliche Verteilung von Expertise hat sich anscheinend nicht durch den Kauf oder die Miete von einfach zu nutzenden Malware-Komponenten – im Sinne von „Malware as a Service“ – kompensieren lassen. Keines der Netzwerkmitglieder operierte mit einem Botnetztyp wie er auf dem Schwarzmarkt hätte beschafft werden können.
Dupont (2013) berichtet, dass die in dem von ihm untersuchten Hackernetzwerk vorhandenen

Monetarisierungsfertigkeiten gleichermaßen begrenzt waren, was auch für den technischen Kopf des Netzwerkes galt, der ebenfalls Schwierigkeiten hatte, eindeutige Gelegenheiten in Geld umzumünzen.
Die erforderlichen sozialen Kompetenzen beinhalten nach Dupont (2013) auch die Fähigkeit, produktive interpersonale Bindungen mittels Computer-vermittelter Kommunikation mit vertrauenswürdigen Komplizen, die man noch nie persönlich getroffen hat, aufzubauen und zu pflegen. Das untersuchte kanadische Hackernetzwerk war durch ein erheblich geringeres Maß an Vertrauen gekennzeichnet, als man vermutet hätte.
Im Ergebnis ist es der mangelhaften Ausprägung von technischen, monetarisierungsbezogenen und sozialen Fertigkeiten zuzuschreiben, dass Hacker-Netzwerke so vergänglich und zugleich auch so angreifbar seitens der Strafverfolgung sind (Dupont, 2013).

4.2.11 Angriffsziele

Woo (2003) hat in einer online-Befragung von Hackern (n=1.385) folgende Angriffsziele erheben können: Mehr als 70% berichteten über Angriffe gegen persönliche Homepages, gefolgt von Angriffen gegen die Webseiten von Universitäten. Die weitere Rangfolge beinhaltete Angriffe gegen die Webseiten kleinerer Firmen (47%), großer Firmen (42%), Webseiten von Regierung und Verwaltung (38%), Pornoseiten (36%), ethnische Seiten (32%), militärische Seiten (28%), Webseiten internationaler Firmen (28%), Webseiten von Nachrichtendiensten (26%), religiöse Webseiten (23%) und Banksysteme (22%).

Herbst (2013) hat im Rahmen einer Sekundäranalyse für das BKA die Angriffsziele von Hacktivisten erhoben. Basierend auf einer Arbeit von Held (2012) lassen sich die Angriffskategorien „politische und staatliche Organisationen“, „Konzerne“ und „weitere“ (Ziele) unterteilen. Gerade Regierungen und deren Vertreter oder staatliche Organe sind immer wieder im Zielspektrum von Hacktivisten zu finden. Gleiches gilt für Unternehmen oder Konzerne, deren Handeln den politischen Vorstellungen von Konzernen widerspricht. Das Spektrum weiterer Ziele ist groß und reicht von Kriminellen, über Rechtsradikale, Sekten bis hin zu Spieleseitenportalen.

Die Ergebnisse einer zum Thema Hacktivismus durchgeführten Fallanalyse (Füllgraf, 2015) entsprechen den Erkenntnissen aus der obigen Sekundäranalyse hingegen nur wenig, was allerdings auch damit zusammenhängen kann, dass die relativ kleine Stichprobe das polizeiliche Hellfeld widerspiegelt, das u. a. durch die Tatwahrnehmung sowie das Anzeigeverhalten der Geschädigten beeinflusst wird. Von 78 Geschädigten aus Deutschland waren lediglich 24% dem Bereich der Privatpersonen zuzuordnen. Bei 21% handelte es sich um Dienstleistungsunternehmen, bei 15% um Vereine/Kirchen und 12% der Geschädigten ließen sich Parteien zuordnen. In weiteren 10% der Fälle waren Schulen und in 9% der Fälle Online-Versandhäuser geschädigt. Eine verhältnismäßig geringe Fallzahl entfiel mit 6% der Fälle auf Behörden und mit 3% auf Produktionsbetriebe.

In dem jüngsten Cyber Security Assessment der Niederlande (NCSC, 2014) wurden den gebildeten Akteurskategorien (vgl. Tabelle 4 in Kapitel 5.1) Angriffsziele zugeordnet. Im Einzelnen waren dies

- bei staatlichen Akteuren („state actors“) Regierungsstellen, Verteidigungsindustrie, die Wirtschaft in den bedeutendsten Sektoren sowie Organisationen, die als Sprungbrett dienen, um andere Ziele anzugreifen
- bei Terroristen Ziele mit einer hohen Wirkung und einer ideologisch-symbolischen Funktion
- bei Berufskriminellen („professional criminals“) Ziele, die Produkte und Dienstleistungen mit vielen Identitäts- oder Finanzdetails liefern
- bei Hacktivisten Nachrichtenorganisationen sowie Ziele mit einem Bezug zur jeweiligen Ideologie. Manchmal sind diese Ziele völlig zufällig gewählt und sind lediglich durch vorhandene Vulnerabilitäten bedingt
- bei Cyber-Vandalen, „script-kiddies“ und Cyberforschern Ziele ganz unterschiedlicher Art
- bei Innentätern sind es aktuelle oder ehemalige Arbeitsumgebungen
- bei der privaten Wirtschaft sind es Wettbewerber, Zivilisten und Kunden.

4.2.12 Arbeitsweisen und -methoden

Bezug nehmend auf Mitnick und Simon (2005; vgl. auch Loper, 2009) unterscheiden Kirwan und Power (2013) vier Hauptmethoden des Hackings:

(1) Technisches Eindringen in Netzwerke

Diese Kategorie meint die Anwendung technischer Werkzeuge, um in fremde Computer und Netze einzudringen. Beispielhaft dafür steht das Portscanning, um herauszufinden, welche Applikationen und Dienste auf einem Rechner laufen und für Angriffe genutzt werden können. Andere Werkzeuge sind bspw. das „paket-sniffing“, in dem Netzwerkverkehr aufgezeichnet und nicht verschlüsselte Daten abgefangen werden oder „password cracker“, um genutzte Passwörter zu erkennen. Typisch sind der Einsatz von Viren oder von sog. „Malware“, um Computer zu schädigen (Kirwan und Power, 2013).

Ziel dieses Berichts ist es nicht, einen Überblick über all diese technischen Angriffsvektoren zu geben. Hier verweisen auch Kirwan und Power (2013) auf zum Teil regelmäßige Veröffentlichungen einer Vielzahl von Sicherheitsunternehmen, Verlagen und öffentlichen Dienstleistern hin, die täterseitige Arbeitsweisen zum Teil hochaktuell und detailliert beschreiben. Bezogen auf Deutschland ist in diesem Kontext insbesondere auf das Bundesamt für Sicherheit in der Informationstechnik (BSI) mit seinen regelmäßig aktualisierten Lageinformatioen, beispielsweise der monatlichen IT-Sicherheitslage oder der Lage der IT-Sicherheit in Deutschland (BSI, 2014) zu verweisen. Diese Informationen stehen interessierten Institutionen zur Verfügung und liegen auch der Polizei vor, so dass keine Notwendigkeit einer Berücksichtigung für diesen Bericht bestand.

(2) „Social engineering“

Die Praktik des „social engineering“ wurde bereits durch die sog. „phone phreaks“

eingeführt. Die Praktik wird auch als Vertrauensbetrug („confidence scam“) bezeichnet (Loper, 2009). Die grundsätzliche Idee des „social engineering“ ist, dass es häufig einfacher und wirkungsvoller ist, potenzielle Opfer zunächst zu täuschen als sie direkt zu bestehlen. Cyberkriminelle überzeugen potenzielle Opfer oder Personen, die den Zugang zu avisierten Opfern verschaffen sollen, mit emotionalen Appellen, die zu Aufregung oder Furcht führen oder sie setzen auf interpersonale Beziehungen, die auf Seiten der zu Täuschenden am Ende zu einem Gefühl von Vertrauen führen oder in eine Verpflichtung münden (Kshetri, 2010). Die Liste an Beispielen ist lang und vielfältig. Beispiele sind

- infizierte Anhänge in E-Mails scheinbar bekannter Personen oder Institutionen,
- Anrufe bei oder persönliches Erscheinen in Firmen mit der Behauptung, Mitarbeiter eines IT-Dienstleisters zu sein, der das Passwort des Netzwerkadministrators benötigt, um einen Fehler im System zu beheben,
- das Abhören der Gespräche von Angehörigen einer Firma oder auch das „shoulder-surfing“, d. h. das heimliche Beobachten von anderen beim Eingeben von Zugangsberechtigungen (Kirwan und Power, 2013; McGuire und Dowling, 2013b).

Die Kombination von Fertigkeiten im Bereich Informationstechnik gekoppelt mit denen des „social engineering“ hilft Hackern, die Wahrnehmung und Entscheidungsprozesse bei potenziellen Opfern durch Vorspielung falscher Tatsachen in ihrem Sinne zu beeinflussen. Beispielhaft dafür ist die Hackerlegende Kevin Mitnick, der es mittels „social engineering“ gelungen war, illegalen Zugang zu Computernetzwerken zu erlangen (Kshetri, 2010).

Kulturübergreifende Kenntnisse und Sprachfertigkeiten helfen social engineers dabei, auch grenzüberschreitend zu agieren. Für Kshetri (2010) ist die Sprachschwelle in Europa eine der größten Barrieren für Cyberkriminelle, gibt es doch über 20 offizielle und etwa 60 regionale und Minderheitensprachen. Nachdem in Staaten, in denen nicht Englisch gesprochen wurde, englischsprachige E-Mails früher umgehend als Phishingversuche gelöscht werden konnten, gehen Kriminelle seit geraumer Zeit dazu über, potenzielle Opfer in ihrer Landessprache zu kontaktieren, was die Detektion erheblich erschwert.

(3) „Dumpster diving“

„Dumpster diving“ (übersetzt: Mülleimertauchen) beschreibt eine Methode, bei der es tatsächlich darum geht, die Mülleimer einer Person oder Firma nach verwertbaren Informationen zu durchsuchen. Das können bspw. Papierschnipsel mit Nutzernamen und Passwörtern aber genauso gut auch alte Datenträger sein (Kirwan und Power, 2013).

(4) „Physical entry“

Sich physisch Zutritt zu verschaffen bedeutet tatsächlich, dass ein Hacker es schafft, Zutritt zu einem Gebäude zu bekommen und einen Hack von innen heraus zu unternehmen. Das kann zum einen passieren, weil Sicherheitssysteme zu lax sind; eine

andere Möglichkeit ist die Anwendung von Methoden des „social engineering“. Ein Hacker muss demzufolge nicht zwingend über besondere technische Fertigkeiten verfügen (Kirwan und Power, 2013).

Chiesa et al. (2009) haben Hacker im Rahmen ihres HPP gefragt, welche Art von Straftaten diese mit ihrem Computer begangen haben. Von den insgesamt 586 Befragten nannten 31% den unberechtigten Zugang zu fremden Computern, gefolgt von dem unberechtigte Kopieren geschützter Programme (25%), der Beschädigung oder Veränderung von Daten oder Programmen (15%), dem Computerbetrug (10%) und Fälschungen (10%).

Chiesa et al. (2009) haben ebenfalls erhoben, ob und warum Hacker eine Signatur mit ihren Hacks hinterlassen. 82% der Befragten (n=250) tun dies nicht gegenüber 18%, die eine Signatur hinterlassen.

Chiesa et al. (2009) haben ferner untersucht, ob Hacker Systemadministratoren warnen würden, wenn sie Vulnerabilitäten entdeckt haben. Lediglich 59% der Befragten haben angegeben, dies zu tun. Dabei ist anzumerken, dass eine solche Warnung zum Teil auch erst im Anschluss an erfolgreiche aber aus Hackersicht folgenlose Attacken erfolgt. 41% der befragten Hacker (n= 253) würden gleichwohl komplett auf Warnungen an Systemadministratoren verzichten.

Interessant ist in diesem Kontext auch die Frage, ob entdeckte Schwachstellen mit anderen geteilt würden. Dazu antworteten 53% der von Chiesa et al. (2009) Befragten (n=231), dass sie diese Erkenntnisse nie teilen würden, wohingegen 32% andere Mitglieder ihrer Hackergruppe informieren würden, aber auch erst, nachdem die zuständigen Systemadministratoren informiert seien. Für das größte Gefahrenpotential stehen die 15% Hacker, die angaben, ihre Entdeckungen und ggf. auch Missbräuche mit anderen Hackern zu teilen und lediglich - im besten Fall - nachträglich Systemadministratoren zu informieren.

4.2.13 Kontakt mit dem Strafjustizsystem

Im Bereich der justiziellen Sanktionen gibt es bislang nur wenige Studien (Broadhurst et al., 2013).

Young et al. (2007) befragten Hacker auf einer DefCon-Konferenz in Las Vegas zu Strafaspekten des Hackens. Die befragten Hacker gingen lediglich von einem geringen Risiko aus, dass es zu einer Bestrafung kommen wird. Das ist insofern bedeutsam, als die Schwere der Strafe kaum einen Effekt hat, wenn die Wahrscheinlichkeit der Bestrafung gering ist, während einer erhöhten Wahrscheinlichkeit der Bestrafung durchaus ein Abschreckungseffekt zugeschrieben wird (Kilias et al., 2009). Young et al. (2007) kamen zu dem Ergebnis, dass Hacker ihren Aktivitäten einen hohen Nutzwert zuschreiben, wobei sie in der Tradition der rational choice-Theorie (vgl. Kapitel 6.4) die Gewinne höher als die potenziellen Verluste bewerten. Aus Sicht von Kirwan und Power dürfte sich das strafbare Verhalten von Hackern nicht verringern, solange diese Ausgangslage nicht grundlegend verändert ist.

In der Befragung von Chiesa et al. (2009) haben lediglich 10% der Hacker (n=223) geantwortet, schon einmal wegen Computerstraftaten inhaftiert bzw. vor Gericht gebracht worden zu sein. 65% der Befragten (n=218) gaben an, diese Möglichkeit nie ernsthaft in Erwägung gezogen zu haben. Hauptgründe dafür waren das angenommene Unvermögen der Ermittler (36%), gefolgt von eigenen Vorsichtsmaßnahmen und eingesetzten technischen

Maßnahmen (35%). Die meisten Befragten zeigten sich zudem herablassend gegenüber Ermittlern und scheinen dem Hacker-Klischee anzuhängen, cleverer und intelligenter als andere zu sein, was in der Konsequenz aus Sicht von Chiesa et al. (2009) oft dazu führt, sich selbst zu exponieren und dem Risiko der Identifizierung auszusetzen.

Chiesa et al. (2009) haben u. a. auch Aspekte des Ausstiegs und eventuellen Wiedereinstiegs in die Szene abgefragt. So wurde u. a. erhoben, ob Hacker nach einem Ausstieg dem Thema erneut „verfallen" sind bzw. irgendwie beteiligt blieben, ggf. auch durch die Arbeit in einer IT-Sicherheitsfirma. Wenigstens 79% der Befragten blieben dem Thema noch irgendwie verbunden („did still dabble in it"), während 21% komplett ausgestiegen sind (n=162). Die Frage, ob Hacking nach einer Zeit der Unterbrechung erneut begonnen wurde, beantworteten 55% positiv und 45% negativ (n=194). Die Autoren werten die Ergebnisse insgesamt so, dass Computerstrafgesetze als Mittel der Abschreckung nicht geeignet sind.

Unter Bezugnahme auf Daten von Marcum et al. (2012) berichten Broadhurst et al. (2013), dass Cyberkriminelle mit am wenigsten zu Haftstrafen verurteilt werden. Daten des US-Justizministeriums für die Jahre 2006 bis 2010 zeigen demnach, dass insgesamt 1.177 Personen für Straftaten aus dem Bereich der Cyberkriminalität verurteilt wurden. Von diesen wurden etwas mehr als die Hälfte (52%) zu Haftstrafen verurteilt, davon 35% zu Strafen unter einem Jahr, 27% zu Strafen zwischen einem und zwei Jahren, 12% zu Strafen bis zu drei Jahren und 19% zu Strafen von über drei Jahren. Bei einer Auswertung der Daten dreier Bundesstaaten lag der Haftanteil bei den Verurteilten mit 65% höher. 62% der Täter waren männlich mit einem Durchschnittsalter von 35 Jahren. Die Stichprobe hatte einen relativ hohen Anteil an Verurteilungen wegen Gewaltstraftaten, was ggf. die höhere Quote der Verurteilung zu einer Haftstrafe erklärt.

Eine Auswertung der Strafen für Computerkriminalität in Australien und Neuseeland zeigte keine signifikanten Unterschiede zwischen Fällen, in denen ein Computer zur Straftatenbegehung genutzt wurde und Fällen, in denen dies nicht der Fall war. Die Strafen für Täter, die Computer nutzten, scheinen ein wenig nachsichtiger ausgefallen zu sein als für diejenigen Täter, die keine Computer nutzten. Die Ergebnisse sollten allerdings mit Vorsicht betrachtet werden, da die ausgewerteten Fälle schon mehr als eine Dekade zurückliegen (ebd.).

4.2.14 Nach der Hacker-Karriere

Turgeman-Goldschmidt (2011) berichtet auf der Basis von Interviews mit israelischen Hackern, dass die Rolle des *„bad" hacker* im Falle eines Ausstieges nicht komplett verlassen wird. Ausgangspunkt dieser Annahme waren Untersuchungen von Ex-Straffälligen, die bei einem Wechsel zu einem konventionellen Lebensstil bisherige Erfahrungen für neue Beschäftigungen im Bereich der professionellen Beratung nutzen (Brown, 1991). In diesem Kontext vergessen Hacker ihre deviante Vergangenheit nicht völlig, sondern transformieren diese in Sozialkapital für ihr neues Leben. Turgeman-Goldschmidt (2011: 44) zeigt am Beispiel eines Hackers, dass Hacker die Risiken ihres Handelns ggf. nur anders kalkulieren, ggf. weniger risikoaffin handeln oder auch aus dem Alter herauswachsen, in dem ihnen Hacken des Hackens wegen Freude bereitet hat („*There' s no longer the fun of 'I can do it*").

Ex-hacker sind nach Turgeman-Goldschmidt (2011) insoweit Menschen, die zum Teil ohne wirkliche Transformation ihre Fähigkeiten für in der Gesellschaft geachtete, weil gesetzestreue Tätigkeiten nutzen. Sie haben keine Probleme mit dem Hacken an sich oder ihrem früheren Leben. Konsequenterweise sind ihre Lebensgeschichten nicht die reformierter Krimineller, sondern eher die von Helden, die die Art sozialer Anerkennung bekommen haben, die sie in den Mittelpunkt stellt.

4.3 Zwischenfazit

Auf der Basis der ausgewerteten Literatur ist von einer jungen Hackerpopulation auszugehen, auch wenn sich das Durchschnittsalter von Hackern in den letzten Jahren vermutlich erhöht hat. Ob man die Tätigkeit des Hackens tatsächlich – wie Yar (2005a) – als typisches Beispiel für die adoleszente Krise interpretieren kann, wäre weitergehend zu untersuchen. Dagegen sprechen sowohl die teilweise sehr frühen Starter als auch ein zunehmend höheres Durchschnittsalter von Hackern. Dass nicht jeder Hacker aus seiner Tätigkeit „herauswächst", könnte auch mit einem Wesenszug zusammenhängen, der u. a. auf Neugier bzw. Wissbegierigkeit und dem Wunsch, technologische Grenzen zu erforschen, fußt. Bedingt wohl auch durch das mehrheitlich junge Lebensalter, leben Hacker häufig noch bei ihren Eltern. Der Anteil an Frauen unter Hackern ist noch immer gering; er scheint in den letzten Jahren allerdings größer geworden zu werden.

Der typische Hacker ist Schüler, Auszubildender oder Student und hat seine Kenntnisse im Bereich Informationstechnik als Autodidakt erworben. Das ist heute einfacher als früher, sind viele junge Hacker doch als sog. „digital natives" mit Computern und dem Internet als Informationsplattform groß geworden. Die meisten Hacker verbringen ihre Freizeit vor allem mit dem Computer und arbeiten viel alleine, ohne dabei sozial auffällig zu sein. Täter unterhalten eher informelle Kontakte, die offenbar eher dem Augenblick als einer soliden Einbindung in soziale Strukturen bzw. Gruppen entstammen. Kontakte werden vor allem über Chats, Cliquen oder als individuelle Freundschaften auch in der realen Welt gepflegt.

Für das Handeln von Hackern scheinen weniger Einzelmotive als Motivbündel ausschlaggebend zu sein. Relevanz haben diesbezüglich der Spaß am Hacken, Unterhaltung und Neugier, genauso wie der Nervenkitzel dabei, etwas Unerlaubtes zu tun. Das Streben zu einer Gruppe Gleichgesinnter zu gehören und durch das Handeln an Achtung und Anerkennung sowie an Status in der eigenen Gruppe bzw. Community zu gewinnen, sind ebenfalls bedeutsame Antriebsgründe, genauso wie der scheinbare Erwerb von Macht durch die Kontrolle fremder und/oder komplexer Systeme. Darüber hinaus dürfen monetäre und politische Gründe als Anreize für Hacker genauso wenig vergessen werden, wie das Streben nach Zerstörung oder Rache.

Um erfolgreich in fremde Computer und Netzwerke einzudringen, ist nicht mehr zwingend ein hohes Fertigkeitsniveau notwendig. Im Netz verfügbare Angebote von „Crime as a Service" oder „Malware as a Service" machen es auch weniger geübten Tätern möglich, Angriffe auf Computer und Netzwerke zu verüben. Die Angriffsziele sind dabei vielfältig. Abhängig insbesondere auch von der jeweiligen Motivation werden Firmen jedweder Größe, Webseiten von Regierung und Verwaltung, Pornoseiten, ethnische oder religiöse Webseiten, Banksysteme oder auch die Webseiten von Privatleuten attackiert (Heise-online, 2015).

Hinsichtlich der Angriffsart können grob vier Herangehensweisen unterschieden werden.

Neben dem direkten technischen Eindringen in Computer und Netze sind dies das „social engineering“ bzw. die Täuschung anderer Personen, um Zugang zu Systemen zu erlangen, das Suchen nach relevanten Informationen im Müll anderer sowie der unberechtigte Zutritt zu IT-Räumen.

Die wenigsten Cyberstraftäter scheinen bereits mit dem Strafjustizsystem in Berührung gekommen zu sein. Mögliche Strafen oder auch Haft sind praktisch ohne Abschreckungswirkung, werden die Kompetenzen und Möglichkeiten der Strafverfolgungsseite doch als nicht besonders hoch eingeschätzt. Eine Rolle dürfte dabei auch die Möglichkeit spielen, infolge der vorhandenen Qualifikationen trotz Straffälligkeit noch Karriere z. B. im IT-Sektor machen zu können, wie einige Hackerlegenden beispielhaft zeigen.

5 Hackertypen

5.1 Entwicklung der Akteurstypisierung

Einen guten Überblick über frühe Versuche, das Spektrum an Hackern zu typisieren, liefert Rogers (2000). Einer der ersten Versuche einer konsistenten Klassifizierung von Hackern stammt demnach von Landreth (1985). Er schlug ein Klassifikationssystem vor, das auf den Aktivitäten der Hacker basierte. Die von ihm festgelegten sechs Kategorien waren: Novize, Schüler/Student, Tourist, Absturzverursacher („crasher“), Dieb. Am wenigsten erfahren waren die Novizen, die einfach Unfug trieben, gefolgt von den Schülern/Studenten, die anstelle ihrer Hausarbeiten in fremde Computer eindrangen. Sie waren intelligent und in der Schule eher gelangweilt. Für den Touristen war Hacken Abenteuer. Was zählte, war Nervenkitzel, in ein System eingedrungen zu sein. Den „crasher“ sah Landreth als destruktiven Hacker, der absichtlich Informationen und Systeme anderer zum Absturz brachte (dazu auch Eckert et al., 1991), während der Dieb Profit aus seinen Aktivitäten zog.

Hollinger (1988) studierte kriminelle Computeraktivitäten in einer Population von Universitätsstudenten. Er schlussfolgerte, dass Hacker eine Entwicklung von Aktivitäten ohne Fachkenntnis bis hin zu in technischer Hinsicht herausragenden Straftaten folgen. Hollinger kategorisierte Hacker in „pirates“, „browsers“ und „cracker“. Während die Piraten die technisch am wenigsten versierte Gruppe bezeichnet, die Urheberrechtsverletzungen begeht, verfügten „browsers“ bereits über mehr IT-Kenntnis, die ihnen Zugang zu den Computern anderer Leute verschafft, ohne dass sie zwingend Daten kopierten oder zerstörten. Aktivitäten der „cracker“ reichten vom Kopieren von Dateien bis hin zur Zerstörung von Programmen und Systemen.

Auf der Basis einer ethnografischen Studie fand Chandler (1996) eine Reihe von Attributen, die für die Kategorisierung von Hackern hilfreich waren: Aktivitäten von Hackern, ihre Hackingfertigkeiten, ihr Wissen, ihre Motivation und die Dauer, d. h. die Zeit, die sie bereits mit dieser Tätigkeit verbracht haben. Chandler kam auf dieser Basis zu einer dreistufigen Klassifikation: Elite („elite group“), Novizen („neophytes“) und Verlierer und Lahme („losers and lamers“). Während die Elite ein herausragendes Maß an Wissen und intrinsischer Motivation besaß, wiesen die Novizen zwar bereits über ein fundiertes Wissensniveau auf, waren jedoch noch in einer Lernphase. Sie waren eher Anfänger und folgten generell der

Gruppe der wirklichen Könner. Die „loosers and lamers“ hingegen zeichneten sich nicht durch besondere intellektuelle Brillanz aus. Ihre Motivation richtete sich auf Profit, Rache, Diebstahl, Spionage etc. Chandler schätzte, dass 30% der Hacker der Gruppe der Elite, 60% den Novizen und 10% den Verlierern und Lahmen zuzurechnen waren.

Nach einer jüngeren Studie von Parker (1998) ließen sich sieben signifikante Profile von Cyberkriminellen bilden: Schlingel bzw. Witzbolde („prankster“), ethische Hardware-Hacker („hackster“), bösartige Hacker („malicious hackers“), persönliche Problemlöser („personal problem solvers“), Karrierekriminelle („career criminals“), extreme Verfechter („extreme advoctes“) sowie Querulanten, Abhängige, irrationale und inkompetente Menschen („malcontents, addicts, and irrational and incompetent people“).

„Hackster“ sah Parker (1998) ähnlich der ersten Hackergeneration, d. h. diejenigen, die die Computer anderer aus Gründen der Bildung, Neugier, unter Wettbewerbsaspekten oder aus irgendwelchen Gründen der sozialen Gerechtigkeit erforschen. „Malicious hacker“ oder „cracker“ sind bösartige Hacker, während „personal problem solver“ tatsächlich nur Probleme lösen wollten, die sie in der realen Welt nicht lösen konnten. In Parkers Befragungen war dies der häufigste Typ. Als „career criminals“ umschrieb er Berufsverbrecher, die ihr Einkommen vollständig oder zumindest in Teilen aus kriminellen Taten zogen. „Extreme advocates“ setzte Parker mit Terroristen gleich; Menschen, die ausgeprägte soziale, politische oder religiöse Meinungen vertraten und versuchen, soziale Bedingungen durch kriminelle Handlungen zu verändern. Die Kategorie der „malcontents, addicts, and irrational and incompetent people“ war die am schwierigsten zu beschreibende Kategorie und ebenfalls schwierigste im Hinblick auf Schutzmöglichkeiten.

Andere Studien unterschieden zwischen externen und internen Angreifern. Letztere Gruppe entfalten illegale Aktivitäten gegen ihre eigene Organisation. Post et al. (1998; zitiert in Rogers, 2000) etikettierten die Gruppe als gefährliche Insider („dangerous insiders“). Diese Personen zeichnen sich u. a. durch einen Mangel an Empathie gegenüber ihren Opfern aus, denen sie zudem die Schuld zuschreiben. Diese Täter glaubten, dass ihre Organisation ihnen spezielle Anerkennung schuldig sei und sie suchen nach Rache, wenn sie diese Anerkennung nicht erfahren (ebd.).

Auf der Basis dieser Klassifizierungen hat Rogers (2000) das in Tabelle 1 abgebildete siebenstufige Unterscheidungssystem für Hacker entwickelt, das im Sinne eines Kontinuums von den niedrigsten technischen Fertigkeiten hin zu den höchsten zu lesen ist. Auch dieses Klassifizierungssystem unterscheidet Hackertypen nicht allein nach ihrem Können, sondern bildet zugleich motivationale Faktoren ab.

Tabelle 1: Hacker-Klassifizierung nach Rogers (2000)

newbie/tool kit	Personen mit begrenzten Computer- und Programmierkenntnissen; verlassen sich bei ihren Angriffen auf fertige Skripte („tool kits“), die sie fertig über das Internet beziehen

cyber-punks	Personen, die bereits über bessere Computer- und Programmierkenntnisse verfügen. Sind bereits in der Lage, begrenzt eigene Programme zu schreiben; haben zudem bessere Kenntnisse von den Systemen, die sie attackieren. Sie schädigen andere wissentlich bzw. bewusst (z. B. durch Webdefacements oder Versand von Junk); viele sind in Identitätsdiebstahl (Diebstahl von Kreditkartendaten) und Betrügereien involviert.
internals	Verärgerte bzw. unzufriedene Mitarbeiter oder Ex-Mitarbeiter, die sich mit Computern gewöhnlich gut auskennen, weil sie ggf. Technologie bezogene Tätigkeiten wahrnehmen/wahrgenommen haben. Können ihre Angriffe infolge ihrer Stellen bezogenen Privilegien ausführen.
coders	Personen, die die Programme schreiben, mittels derer andere Hacker Computer angreifen und infiltrieren.
old guard hackers	Personen, die keine kriminellen Absichten zu hegen scheinen, obwohl es eine beängstigende Missachtung persönlichen Eigentums gibt. Diese Gruppe vertritt ideologisch die Hacker der ersten Generation, die insbesondere die intellektuelle Anstrengung reizte.
professional criminals	Berufskriminelle und Cyberterroristen stellen wahrscheinlich die gefährlichsten Gruppen dar. Sie sind spezialisiert in Industrie- bzw. Wirtschaftsspionage, sind gemeinhin gut ausgebildet und haben Zugang zu modernster-Ausrüstung
cyber-terrorists	

Eine Gesamtübersicht der bis zum Jahr 2000 publizierten Typisierungen von Hackern liefert die nachfolgende Tabelle 2.

Tabelle 2: Kategorisierungen von Hackertypen bis zum Jahr 2000 (vgl. Woo, 2003: 12)

Landreth (1985)	**Hollinger (1988)**	**Goodell (1996)**	**Chandler (1996)**	**Chantler (1996)**	**Power (1998)**	**Parker (1998)**	**Adamski (1999)**	**Rogers (2000)**
Novice	Pirates	Hackers	First generation	Neophytes	Sport intruders	Pranksters	The elite	Newbie/ toolkit (NT)
Student	Browsers	Crackers	Second generation	Losers & lamers	Competitive intelligence	Hacksters	Ordinary	Cyberpunks (CP)
Tourist	Crackers	Phreakers	Third generation	Elite group	Foreign intelligence	Malicious hackers	Darksiders	Internals (IT)
Crasher			Fourth generation			Personal problem solvers		Coders (CD)
Thief						Career criminals		Old guard hackers (OG)
						Extreme advocates		Professional criminals (PC)
						Malcontents, addicts, and irrational & incompetent people		Cyber-terrorists (CT)

Rogers hat seine o. g. häufig zitierte Hackertaxonomie (u. a. Fötinger und Ziegler, 2004; Furnell, 2002; Woo, 2003) nachfolgend mehrfach überarbeitet. In einer späteren Arbeit unterscheidet er folgende acht „Primärklassifikationen“ (Rogers, 2005):

(1) Novizen bzw. Anfänger („Novices“)
(2) „Cyber-Punks“
(3) Innentäter („Internals“)
(4) kleine Diebe („Petty Thieves”)
(5) Virenschreiber („Virus Writers”)
(6) Hacker alter Garde („Old Guard hackers“)
(7) Berufskriminelle („Professional Criminals”)
(8) Cyberkämpfer („Information Warriors“).

Vor dem Hintergrund, dass einige der Kategorien bereits beschrieben wurden bzw. noch beschrieben werden (vgl. Kapitel 5.2) sei an dieser Stelle lediglich auf die Kategorie der „kleinen Diebe“ kurz eingegangen: Für diese Gruppe ist Hacking ein Mittel, bestehende kriminelle Aktivitäten auszuweiten (Parker, 1998). Diese Täter wollen ausdrücklich keine Berühmtheit durch ihr Hacken erlangen, wäre dies doch kontraproduktiv für das Geschäftsmodell. Der Bezug zu Technologie und Internet resultiert allein daraus, dass auch traditionelle Ziele einen größeren Technologiebezug bekommen haben (wie z. B. Banken, Kreditkarten).

Chiesa et al. (2009) haben im Rahmen ihres Hacker Profiling Project (HPP) eine Kategorisierung von Hackern vorgenommen, die im Wesentlichen auf in der Literatur berichteten Unterscheidungssystemen wie dem von Rogers (s. o.) beruht. Die in Tabelle 3 im Detail dargestellte Typisierung differenziert damit ebenfalls nicht allein nach den Fertigkeitsniveaus von Hackern, sondern bildet zugleich Motivationen ab:

Tabelle 3: Hacker-Klassifizierung nach Chiesa et al. (2009)

wannabe lamer	Als die amüsanteste Variante bezeichnet, die praktisch überall im Netz zu finden ist und konstant und öffentlich nach Hilfe und Beschreibungen ruft.
script-kiddie	Kulturell fortgeschritten, jedoch auf Anleitungen anderer angewiesen, um Systeme anzugreifen und später damit prahlen zu können. Anm.: Beinhaltet die ursprünglich eigene Gruppe der „*37337 K-rAd iRC #hack 0-day Exploitz" Guys*", die alles dafür tun würden, Ruhm zu erlangen, allerdings wie die „script-kiddies" auf bereits verfügbare Angriffswerkzeuge zugreifen, statt diese selber zu entwickeln.
cracker	Ursprünglich diejenigen, die den Schutz kommerzieller Software außer Kraft gesetzt haben. In jüngerer Zeit interpretiert als „gewalttätige" Hacker, die sich freuen, wenn sie zum Albtraum von Systemadministratoren werden, weil sie Daten löschen und dauerhaft Schaden verursachen. Verfügen über das Wissen, selber Angriffstools zu entwickeln. Bleiben so lange wie möglich in fremden Systemen; löschen alle Spuren beim Ausstieg. Gefährliche Hacker-Kategorie.
ethical hacker	Diejenigen, die zwar widerrechtlich in fremde Systeme eindringen und erforschen, rechtmäßige Inhaber jedoch ggf. auf erkannte Schwachstellen hinweisen. Arbeiten nicht für Geld oder Ruhm, sondern aus Leidenschaft.
quiet, paranoid, and skilled hacker	Gefährlichster der nicht Geld-orientierten Hacker. Mit hoher Kompetenz ausgestattet, erforscht er - möglichst ohne entdeckt zu werden - Systeme. Hat kein Interesse daran, anderen zu imponieren und wird im seltenen Fall, dass seine Präsenz in einem System bekannt wird, sofort verschwinden.
cyber-warrior	Söldner mit hoher Kompetenz, die ggf. ursprünglich aus einer der o. g. Kategorien stammen. Agieren vorsichtig und zurückhaltend und attackieren kaum multinationale Konzerne, sondern eher Internet Service Provider, Universitäten, Ämter etc. Arbeiten für Geld oder Ideale.
industrial spy	Arbeiten rein für Geld. Hoch qualifiziert mit viel Erfahrung; gefährlich, wenn auf der Suche nach vertraulichem Material. Insider

	gehören ebenfalls zu dieser Kategorie. Zahl dieser Täter soll über die letzten Jahre[3] angesichts der hohen Zahl an „white-collar"-Straften exorbitant gestiegen sein.
government agent	Verfügen über eine guten Hacking-Hintergrund und werden für Zwecke der Spionage, Gegenspionage sowie des Informations-Monitorings von Regierungen, Individuen, terroristischen Gruppierungen und strategisch relevanten Industrien beschäftigt.
military hacker	Anm.: Kategorie, die ursprünglich nicht bestand, sondern erst im Laufe des Projektes aufgenommen wurde. Deckt den zunehmenden militärischen Anteil im Bereich Hacking ab.

Chiesa et al. (2009) haben sich über die in Tabelle 3 wiedergegebene Klassifizierung auch mit dem häufig genannten Unterscheidungssystem von Hackern in sog. „white-hats"-, „black-hats"- und „grey-hats" befasst, das von der Basis her ein motivationales Unterscheidungssystem darstellt, welches nachfolgend erläutert sei.

(1) „White-hats"

Die Bezeichnung wird in Anlehnung an die gesetzestreuen Darsteller in Cowboyfilmen genutzt, die regelmäßig weiße Hüte trugen. In dem aktuellen Kontext werden damit die Personen umschrieben, die gerne mit dem Computer arbeiten und ggf. auch fremde Systeme infiltrieren, dabei allerdings keine Schäden verursachen. „White-hats" werden z. T. auch als „ethical hackers" bezeichnet, wobei letzterer Begriff gemeinhin mehr auf eine Gruppe von Beschäftigten oder Beratern angewendet wird, deren spezifischer Auftrag es ist, sog. „exploits", also angreifbare Schwachstellen bzw. Systemfehler zu finden, um Systeme sicherer zu machen (Kirwan und Power, 2013). „White-hats" hacken im Rahmen des gesetzlichen Rahmens, kooperieren mit Autoritäten wie der Polizei, arbeiten als Berater für Regierungen und Unternehmen und sind an Aktionen zur Bekämpfung der Computerkriminalität beteiligt (Chiesa et al., 2009).

(2) „Black-hats"

Der Begriff „Black-hat" bezeichnet im Gegensatz dazu nur solche Hacker, die mit ihrem Tun absichtlich in irgendeiner Art und Weise Schädigungen verursachen bzw. die unabhängig von eventuellen Schäden unautorisiert Zugang zu Informationen oder Software erlangen. Das Eindringen in Informationssysteme, um ihnen ihre Geheimnisse zu entreißen bzw. Informationen zu stehlen und auch zu verkaufen, ist ihr normales Geschäft (Chiesa et al., 2009). Ein Synonym für den Begriff ist „Cracker".

(3) „Grey-hats":

Der Begriff umschreibt schließlich die Grauzone derjenigen Hacker, die ihr erlangtes Wissen über Systemschwachstellen nur unter bestimmten Bedingungen – häufig gegen Geld – den Verantwortlichen zur Verfügung stellen. In einigen Fällen bezeichnet „grey-hat"-Hacking auch Angriffe gegen aus ethischer Sicht dubiose Personen oder Organisationen (Kirwan und Power, 2013). Aus Sicht von Chiesa et al. (2009) handelt

[3] Bezieht sich auf das Referenzdatum der Buchveröffentlichung 2009.

es sich bei den „grey hats“ um diejenigen Hacker, die sich weder als weiß noch schwarz etikettieren lassen wollen; man könnte sie genauso gut „pink-hats“ nennen oder eine andere Farbe willkürlich wählen. Hintergrund ist, dass sich diese Gruppe mit keinem der Label identifiziert, weil ihr Handeln weder komplett gut noch schlecht ist. Sie folgen wenig rigiden ethischen Orientierungen, sondern nehmen ggf. auch stimmungsabhängig oder situationsbedingt schädigende oder auch eher nicht schädigende Hacks vor (Holt, 2010 & 2014).

Chiesa et al. (2009) haben dieses Unterscheidungssystem, das sich ursprünglich wohl allein auf sachkundige bzw. qualifizierte („skilled“) Hacker bezog (Holt, 2014), in einem weiteren Schritt mit fertigkeits- sowie tätigkeitsbezogenen Merkmalen kombiniert. Die so gebildeten Unterkategorien umfassen bei den „black-hats“ z. B. die „black-hat script-kiddies“. Diese wiederum beinhalten Unterkategorien wie „basic coders“, d. h. Programmierer auf unterster Ebene, die in der Lage sind, vorhandenen Code zu manipulieren, um damit neue Exploits auszuprobieren. Auf Werkzeuge zur Entwicklung und Ausführung von Attacken wie Metasploit sind sie dennoch angewiesen. „Full-blown coders“ sind im Gegensatz dazu in der Lage, ihren eigenen Code zu schreiben.

„Script-kiddies“ werden an einer anderen Stelle im Text zwar als keine wirklichen „black-hats“ bezeichnet, seien allerdings in der Lage, Programmierfehler auszunutzen und so „’black’ high-impact actions“ auszuführen. Beispiel dafür war der ‚Melissa’-Wurm in seiner ersten Ausführung (vgl. Chiesa et al., 2009: 48). Andere Unterkategorien bei den „black-hats“ sind die „firebug hacker“ bzw. „arsonist hackers“, die sich bei großen Attacken quasi mitten im Sturm bewegen und sich an den Emotionen der Geschädigten weiden, sowie die „skill testing hackers“, die in angegriffenen Systemen Checklisten abarbeiten, um bestimmte Dinge zu verifizieren. Gefährlichste und aggressivste Untergruppe sind nach Chiesa et al. (2009) die „legal black hatters“, die auf vertraglicher Basis Informationssysteme zerstören.

Unterkategorien finden sich auch bei den „grey-hats“. Hier werden neben den traditionellen „grey-hats“ ebenfalls die „skill testers“ genannt, die allenfalls über die Motivlage und die angewendeten Methoden von der gleichen Untergruppe bei den „black hats“ abgrenzbar sind. Schafe oder „sheeps“ werden eine weitere Unterkategorie bei den „grey-hats“ genannt, die hochangesehenen Hackern einfach folgen, ohne deren Handlungen oder Entscheidungen wirklich zu verstehen (ebd.).

Eigene Wege der Differenzierung von Hackern, die nicht aus den o. g. zumeist angelsächsischen Versuchen abgeleitet sind, finden sich in der deutschen Literatur:

Vick und Roters (2003) haben in ihrer Analyse von deutschen Tatverdächtigen im Bereich „Account-Missbrauch“ (n=599) drei Tätertypen herausgearbeitet. Der typische Täter ist demnach männlich, 16 bis 21 Jahre alt, lebt bei den Eltern, handelt aus Bereicherungsabsicht oder schlicht, um Dinge auszuprobieren. Er verfügt über eine mittlere bis gehobene Schulbildung sowie mittlere bis hohe Computerkenntnisse. Er ist Schüler oder Auszubildender, hat seine IT-Kenntnisse als Autodidakt erworben und beschäftigt sich viel mit dem Computer. Seine Freizeit verbringt er vor allem in Cliquen, mit dem Konsum von Filmen bzw. Videos und Musik und nicht oder nur wenig mit Vereinsaktivitäten. Auf Tatmöglichkeiten wurde er durch Chats aufmerksam. Täter unterhalten eher informelle Kontakte, die offenbar eher dem Augenblick als einer soliden Einbindung in soziale

Strukturen entstammten. Kontakte wurden vor allem über Chats, Cliquen oder individuelle Freunde gepflegt. Vick und Roters (2003: 36) bezeichnen diese Tätergruppe als „hoch individualisiert“. Vick und Roters (2003) haben darüber hinaus einen zweiten, eher untypischen Tätertyp analysiert, der älter und ebenfalls männlich ist, während sie in einem dritten Typ weibliche Täter zusammenfassen.

Rheinberg und Tramp (2006) haben in einer online-Befragung in Deutschland eine gezielt rekrutierte Stichprobe besonders engagierter Computernutzer (n=271) zu den Anreizen freizeitlicher Computernutzung befragt. Auf der Basis von Literaturanalysen und Expertenbefragungen haben sie unterschiedliche Nutzungsweisen analysiert und drei grobe Nutzertypen mit folgender Verteilung herausarbeiten können:

(1) Zweckorientierte Nutzer: 58% der Befragten ließen sich dieser Kategorie von Computernutzern zuordnen, für die der Rechner die Funktion eines Werkzeuges besitzt, welches auch in der Freizeit genutzt wird, um etwas abzuarbeiten bzw. zu erledigen (Textverarbeitung, Rechnen, Mails, Datenrecherchen, Bild-/Fotobearbeitung etc.).

(2) Hacker: 22% ließen sich dieser Kategorie von Personen zuordnen, die ohne Schädigungsabsicht in fremde Systeme eindringen, ob diese nun geschützt oder ungeschützt sind. Diesen Personen geht es um die Beschaffung oder Veröffentlichung von Informationen; sie haben nicht das Ziel, Schäden zu verursachen.

(3) Cracker: 20% ließen sich dieser Kategorie von Personen zuordnen, die – wie Hacker – in fremde Systeme eindringen und dort allerdings nachteilige Effekte oder Schaden bewirken wollen (bspw. in dem Viren, Würmer oder sonstige Angriffswerkzeuge eingesetzt werden).

Insgesamt zeigen die Befunde sowohl hinsichtlich des Gesamtprofils der bevorzugten Computernutzung als auch hinsichtlich der Anreize zur Computerinteraktion deutliche Unterschiede zwischen Hackern und Crackern, auch wenn sich das Erforschen und Zerstören fremder Systeme keinesfalls ausschließen. Auch Flow-Erlebnisse (vgl. dazu Kapitel 6.7) finden sich sowohl bei hacker- als auch bei crackerspezifischen Aktivitäten, was die Autoren durchaus positiv interpretieren: „Er (der Crackertypus) könnte sich genauso gut in die eher leistungsmotivierten Hackeraktivitäten vertiefen“ (Rheinberg und Tramp, 2006: 26).

Eine differenzierte Typisierung von Hackern einschließlich der Beschreibung von Fertigkeitsniveaus und Zielrichtungen unterschiedlicher Tätertypen wird seit einigen Jahren durch das niederländische National Cyber Security Centre in Zusammenarbeit mit dem öffentlichen Sektor (u. a. Polizei, Nachrichtendienste, Justiz), wissenschaftlichen Institutionen und dem privaten Sektor als Teil einer umfassenden Bewertung der niederländischen Sicherheitslage vorgenommen. Augenscheinliches Ziel dieser Bewertung ist die Bereitstellung eines deutlichen und möglichst vollständigen Einblicks in Veränderungen niederländischer „Interessen”, die verletzt werden könnten, der Bedrohungen und des Ausmaßes an Resilienz, über das die niederländische Gesellschaft im Bereich der Cybersicherheit verfügt (vgl. NCSC, 2012, 2013, 2014).

Eine Übersetzung der jüngsten, 2014 erstellten, Bedrohungsmatrix identifizierter Tätertypen findet sich in nachfolgender Tabelle 4:

Tabelle 4: Bedrohungsmatrix (NCSC, 2014: 9).

Bedrohungsquelle	**Ziele**		
	Regierungen	**Privatwirtschaft**	**Bürger**
Staatl. Akteure	Digitale Spionage	Digitale Spionage	Digitale Spionage
	Offensive Cyberfähigkeiten	Offensive Cyberfähigkeiten	
Terroristen	Unterbrechung/ Übernahme von IT	Unterbrechung/ Übernahme von IT	
Berufsverbrecher	Diebstahl und Veröffentlichung oder Verkauf von Informationen ⇩	Diebstahl und Veröffentlichung oder Verkauf von Informationen	Diebstahl und Veröffentlichung oder Verkauf von Informationen ⇧
	Manipulation von Informationen ⇩	Manipulation von Informationen ⇩	Manipulation von Informationen
	IT-Störungen ⇧	IT-Störungen ⇧	IT-Störungen ☆
	Übernahme von IT ⇩	Übernahme von IT ⇧	Übernahme von IT
Cybervandalen und Skriptkiddies	Informationsdiebstahl ⇩	Informationsdiebstahl ⇩	Informationsdiebstahl
	IT-Störungen ⇩	IT-Störungen	
Hacktivisten	Diebstahl und Veröffentlichung von Informationen	Diebstahl und Veröffentlichung von Informationen	Diebstahl und Veröffentlichung von Informationen
	Defacement	Defacement	
	IT-Störungen	IT-Störungen	
	Übernahme von IT ☆	Übernahme von IT	
Innentäter	Diebstahl und Veröffentlichung oder Verkauf von Informationen	Diebstahl und Veröffentlichung oder Verkauf von Informationen	
	IT-Störungen	IT-Störungen	
Cyberforscher	Erhalt und Veröffentlichung von Informationen	Erhalt und Veröffentlichung von Informationen	
Privatwirtschaft		Informationsdiebstahl (Industriespionage) ⇩	Kommerzielle Nutzung bzw. Missbrauch oder „Wiederverkauf“ von Informationen ☆
Kein Akteur	IT-Fehler/-Versagen	IT-Fehler/-Versagen	IT-Fehler/-Versagen

Legende:

Niedrig	Mittel	Hoch
Neue Trends/Phänomene ODER (ausreichend) Maßnahmen zur Beseitigung der Bedrohung ODER keine wesentlichen Zwischenfälle im Berichtszeitraum	Neue Trends/Phänomene ODER (begrenzte) Maßnah-men zur Beseitigung der Bedrohung ODER Zwischenfälle zumeist außerhalb der NL	Deutliche Entwicklungen, die die Umsetzung von Bedrohungen begünstigen ODER Gegenmaßnahmen haben lediglich begrenzte Wirkung ODER Zwischenfälle in den NL

Bedrohung hat zugenommen ⇧, abgenommen ⇩; neue Bedrohung ☆

5.2 Ausgewählte Akteurskategorien

In dem nachfolgenden Abschnitt werden (insbesondere) die in Tabelle 4 genannten Akteurskategorien kurz beleuchtet, die noch nicht besprochen wurden. In dieser primär aus politisch-strategischer Sicht erfolgten Kategorisierung geht es im Kern nicht um definitorische Feinabstufungen von Angreifertypen. Ziel ist eher, voneinander möglichst gut abgrenzbare Akteurskategorien zu bilden, um einen Überblick über mögliche Angriffsziele und Gefährdungspotenziale zu bekommen und auf dieser Basis dann ggf. auch Gegenstrategien erarbeiten zu können.

5.2.1 Staatliche Akteure

Staatliche Akteure ("State actors") sind qua Definition Akteure, die nationalen Regierungen zugerechnet werden müssen. Die Bedrohung resultiert aus der Absicht, die eigene geopolitische Situation (z. B. in diplomatischer, militärischer oder wirtschaftlicher Hinsicht) zu verbessern. Staaten sind sich seit einigen Jahren der Signifikanz der Cyberdomäne bewusst und entwickeln bzw. investieren daher in diesem Feld. Bereits vor einer halben Dekade war davon auszugehen, dass zwischen 100 und 120 Staaten Cyberangriffsstrategien und „infowar"-Fähigkeiten entwickeln (Kshetri, 2010).

Nach dem jüngsten Cyber Security Assessment der Niederlande werden staatlich gesteuerte Hacker („state actors") neben Berufsverbrechern („professional criminals") in dem Feld als die größte Bedrohung wahrgenommen. Sowohl der AIVD (Allgemeiner Nachrichten und Sicherheitsdienst der Niederlande) als auch sein militärischer Pendant MIVD haben festgestellt, dass sich die Bedrohung durch digitale Spionage zwischen April 2013 und März 2014 nicht verändert hat. Fast alle internationalen Nachrichtendienste haben ihre digitalen Fähigkeiten in den letzten Jahren ausgebaut, so dass zwischenzeitlich auch ärmere Länder zu digitalen Angriffen in der Lage sind (NCSC, 2014).

Staaten sollen im Vergleich zum letzten Jahr besser entwickelte und komplexere Angriffstechniken verwenden. Die niederländischen Dienste AIVD und MIVD haben beobachtet, dass Angreifer ihre Ziele in einem steigenden Maße spezifisch infizieren und auch versuchen, Datendiebstähle im Rahmen des regulären Netzwerkverkehrs zu verschleiern. Dies wiederum macht Spionageangriffe schwer erkennbar (NCSC, 2014).

In den letzten Jahren wurde zudem festgestellt, dass sich Hackerkollektive selber als Verteidiger staatlicher Interessen gerieren. Beispielhaft dafür stehen pro-russische und pro-ukrainische Hacker, die während der Krim-Krise auf der jeweils anderen Seite DDoS-Attacken und Webdefacements ausgeführt haben. AIVD und MIVD haben Anzeichen dafür gefunden, dass diese Hacker in ihrem Tun nicht nur toleriert, sondern ggf. sogar staatlich unterstützt werden, wobei die Beziehungen insgesamt ein wenig zwielichtig erscheinen. Gegen die Niederlande wurden derartige Angriffe im letzten Jahr allerdings nicht festgestellt (NCSC, 2014).

Gaycken (2014) weist im Kontext staatlicher Akteure auf die Gefahr einer viel stärkeren Verbreitung von Offensivwissen hin. Insbesondere bei den Militärs und den Nachrichtendiensten gibt es weltweit das Bemühen, die sog. „wizards", also diejenigen Hacker zu gewinnen, die nicht nur einfach Angriffswerkzeuge nachbauen, sondern selber über

ein profundes Systemwissen verfügen. Deren Wissen soll methodologisiert werden, um es dann seinen anderen Truppen beibringen zu können. Gaycken (2014) weist zudem auf existierende Befürchtungen hin, dass Staaten Cyberangriffe als Terrorangriffe tarnten, um so bestimmte Reaktionen zu provozieren – sogenannte Operationen unter falscher Flagge.

5.2.2 Cyber-Terroristen

Terroristen agieren aus ideologischer Perspektive, um bspw. sozialen Wechsel zu initiieren, Furcht in der Bevölkerung zu streuen oder um politische Entscheidungen zu beeinflussen. In ihrem Handeln haben sie keine Gewissensbisse welcher Maßnahme auch immer gegenüber. Genutzt werden zielgerichtete Gewalt gegen Menschen bzw. Unternehmen (NCSC, 2012).

Kshetri (2010) führt aus, dass es Cyber-Terrorismus aus Sicht der Experten zumindest noch 2002 kaum gab, wobei einige Jahre später von wenigstens 4.300 Webseiten berichtet wird, die Terroristen und ihren Unterstützern dienen. Die amerikanische CIA ging 2007 davon aus, dass es zumindest zwei terroristische Organisationen gab, die die Fähigkeiten und Qualifikationen besitzen und bei denen damit gerechnet werden müsse, dass sie Cyberangriffe gegen die amerikanische Infrastruktur fahren (ebd.). Ein Jahr später wurde in einem Artikel des Economist gefragt „*Why bomb your enemy's power stations or stockmarkets if you can disable them with software?*" (Kshetri, 2010: 14).

Bezogen auf die Niederlande hat sich die Bedrohung durch von Terroristen verursachte Cyberattacken seit der Veröffentlichung des dritten „Cyber Security Assessment Netherlands" im Jahre 2013 nicht verändert. Nach der aktuellen Lagebeschreibung verfügen Terroristen bislang nicht über adäquate Fertigkeiten und Mittel, um wirklich sozial zerstörerische Schäden zu verursachen. Jihadisten bspw. haben bislang lediglich kleinere und einfachere Cyberattacken (Defacements und DDoS-Attacken) in den Niederlanden und woanders verübt. Die u. a. im Zusammenhang mit Informationserhebungen oder der Durchführung von Propagandaaktivitäten gewonnene technische Expertise insbesondere von Jihadisten beinhaltet allerdings die Gefahr der Begehung schwerer und versierterer Cyberangriffe in der Zukunft (NCSC, 2014).

5.2.3 Berufsverbrecher

Aus niederländischer Sicht haben sich aus Gewinnabsicht handelnde Berufsverbrecher („professional criminals") im letzten Jahr verstärkt Angriffen gegen die Infrastruktur des Internets als dem Missbrauch individueller Computer oder Websiten zugewandt. Der Missbrauch z. B. eines Service-Providers, eines Domain-Name-Servers oder einer populären Website bieten aus Tätersicht erheblich größere wirtschaftliche Ertragschancen als der Angriff auf individuell kompromittierte Websites (NCSC, 2014).

Diese Täter werden aus niederländischer Sicht neben den staatlich gesteuerten Hackern („state actors") als größte Bedrohung angesehen. Dabei wird darauf verwiesen, dass kriminelle Organisationen nicht nur immer professioneller werden; auch das Feld krimineller Dienstleistungen („professional criminal services"), auf deren Entwicklung bereits seit einigen Jahren verstärkt hingewiesen wird, wird immer besser sichtbar. Als struktureller

Bestandteil der Cybercrime ermöglichen es diese am Markt angebotenen Dienstleistungen auch weniger erfahrenen bzw. schlechter ausgestatteten Kriminellen, ausgefeilte Cyberattacken auszuführen bzw. mit ihnen zu drohen. Beispielhaft dafür wird das Erscheinen der Ransomware CryptoLocker gesehen. Relativ gesehen resultiert dabei ein großer Teil der Cyberkriminalität aus den Ländern, in denen die Behörden nur in begrenztem Maße Cyberkriminalität bekämpfen bzw. zu verhindern suchen (NCSC, 2014).

5.2.4 Cybervandalen und „script-kiddies“

Mit Cybervandalen und „script-kiddies“ umschreiben die Cybersicherheitsanalysen der niederländischen Regierung (NCSC, 2012, 2013, 2014) letztlich zwei unterschiedliche Kategorien: Cybervandalen verfügen über ein fundiertes IT-Wissen und entwickeln ihre eigenen Werkzeuge bzw. entwickeln diese weiter. Ihre Motive sind weder finanzieller noch ideologischer Art. Sie führen Hacks aus, weil sie es können und anderen dies demonstrieren wollen.

Die sog. „script-kiddies“ sind in diesem Bericht bereits mehrfach angesprochen worden. Sie verfügen lediglich über ein begrenztes IT-Wissen, nutzen öffentlich bekannte Schwachstellen aus und verwenden von anderen entwickelte Werkzeuge (Robertz und Rüdiger, 2012). Oft handelt es sich um junge Menschen, denen die Folgen ihres Handelns nur unzureichend klar sind. Sie wollen entweder Spaß auch auf Kosten anderer haben, streben aber auch danach, böswillig Schaden anzurichten (NCSC, 2012; ZDNet, 2015). Loper (2009) bezeichnet sie als Hacker, die nach der leichten Tötung („easy kill“) streben. Sie suchen nicht nach spezifischen Informationen oder spezifischen Hackingzielen, sondern erhalten ihre Gefährlichkeit durch die eher zufällige Auswahl von Zielen, so dass sie auch als Plage bzw. Pestilenz des Internets verschrien sind.

5.2.5 Hacktivisten

Der Hacktivismus stellt eine Verbindung der Konzepte des Hackings und des politischen Aktionismus dar (Füllgraf, 2015; Samuel, 2004). Es geht um die Durchsetzung bestimmter politischer wie sozialer Ziele mit Mitteln der Informationstechnik. Hacktivisten setzen Hacking-Tools u. a. für Protest- wie Propagandazwecke ein und zeigen keine Profitorientierung (Füllgraf, 2015). Über diesen relativ groben Definitionsversuch hinaus ließe sich der Begriff des Hacktivisten weiter differenzieren. So unterscheidet Herbst (2013) auf der Basis einer Differenzierung von Samuel (2004) in einer für das BKA durchgeführten Sekundäranalyse zum Thema „Hacktivismus“ allein drei Unterformen: politische Cracker, normorientierte (performative) Hacktivisten und politisch codierende Hacktivisten. Herbst grenzt zudem sog. Internetaktivisten oder Cyberaktivisten von Hacktivisten ab (ebd.).

5.2.6 Innentäter

Innentäter repräsentieren aus Sicht von Rogers (2005) das größte Risiko, auch wenn es sich tendenziell um die am wenigsten publizierte Hackerkategorie handelt. Sowohl aus Wirkungs- wie auch aus Kostensicht können sie als die teuersten Täter bezeichnet werden (Randazzo, 2004). Die Gruppe besteht primär aus verärgerten bzw. unzufriedenen Mitarbeitern oder Ex-

Mitarbeitern, die sich mit Computern gewöhnlich gut auskennen, weil es sich häufig um IT-Fachkräfte, bspw. Administratoren handelt.

Nach Lowman (2010) sind Insider-Attacken quantitativ bzw. in Bezug zu Attacken von außen nur schwer abzuschätzen, was auch damit zusammenhängt, dass Unternehmen gerade Insider-Attacken kaum anzeigen würden, weil sie eine Beschädigung ihres Renommees befürchten oder aber der Schaden zu gering war. Zudem seien Insider-Attacken schwieriger zu identifizieren als Attacken von außen.

Kshetri (2010) berichtet unter Bezugnahme auf einen FBI-Bericht aus 2006, dass mehr als 40% aller Angriffe aus dem Innenbereich einer Organisation resultieren. Ähnlich sind die Ergebnisse einer Befragung irischer Geschäftsleute, wonach etwa 40% der Befragten angaben, dass interne Cybercrime-Ermittlungen dazu geführt hätten, Mitarbeiter zu entlassen bzw. dass diese kündigen (ebd.). Nach anderen Quellen sind sogar 70% der Fälle unberechtigten Computerzugangs, die zu einem Verlust führten, auf Insider zurückzuführen (ebd.).

Nach dem Data Breach Investigations Report 2015 von Verizon steht der „Missbrauch durch Insider“ für fast 21% der 2014 registrierten Sicherheitsvorfälle (Verizon, 2015). In 55% der Fälle von Insidermissbrauch handelte es sich um Privilegienmissbrauch, d. h. interne Akteure missbrauchen den Zugang, der ihnen anvertraut wurde, um sensible Daten unrechtmäßig zu erlangen oder weiterzugeben. Am häufigsten betroffen waren auch hier die öffentliche Verwaltung, der Gesundheits- und Finanzsektor. Motive sind dabei in 40% der Fälle finanzieller Art bzw. betreffen sonstige Annehmlichkeiten oder Vorteile (ebd.).

Nach dem 2015-Cyber-Security-Intelligence-Index von IBM waren Insider im Jahr 2014 für mehr als die Hälfte (55%) aller Cyberattacken auf Unternehmen verantwortlich. Die täterseitige Analyse nennt als Angreifer ehemalige Angestellte, Dienstleister mit Systemzugriff sowie Mitarbeiter als Opfer von Kriminellen. Dabei geht ein knappes Viertel (23%) der Attacken auf Anwenderfehler zurück, etwa wenn sie präparierte Links in Spam-E-Mails anklicken, während böswillige Insider für fast ein Drittel (31%) der Fälle stehen (IBM 2015).

5.2.7 Cyberforscher

Cyberforscher sind hier in dem Sinne gemeint, dass es sich um Forscher handelt, die nach Schwachstellen in der IT suchen, um letztlich zur Verbesserung der IT-Sicherheit beizutragen. Das Fertigkeitsniveau dieser Forscher variiert. Sie nutzen häufig die Medien, um ihre Erkenntnisse regelmäßig nach Einräumung einer Frist zur Nachbesserung oder Stellungnahme zu publizieren und zur Sensibilisierung beizutragen. Gerade die Veröffentlichung von Schwachstellen bspw. im Rahmen von (internationalen) Hackerkonferenzen kann jedoch zumindest temporär auch zu einer erhöhten Vulnerabilität von Regierungseinrichtungen wie auch Unternehmen führen. Zur Vermeidung eigener Strafbarkeit haben öffentliche wie private Träger sog. „responsible disclosure“-Leitfäden[4] veröffentlicht (NCSC, 2014).

[4] Vgl. in DEU bspw. „Praktischer Leitfaden für die Bewertung von Software im Hinblick auf den § 202c, StGB – Leitfaden“ des Bitkom (2008): https://www.bitkom.org/files/documents/Hackertools_web_haftung_%282%29.pdf

5.3 Sonstige Akteurskategorien

Zusätzlich zu den bislang genannten Differenzierungen sind im letzten Jahrzehnt eine Reihe weiterer Hackertypen klassifiziert worden. Beispielhaft sei der „microserf“ genannt, den Taylor (2000) als einen Hackertypen beschrieben hat, der zwar noch über Verbindungen zu Hackergruppierungen verfügt, nun allerdings in Unternehmensstrukturen tätig ist. Shinder (2002) hat jugendliche Hacker, die insbesondere Spaß haben wollen, in vier Kategorie unterteilt, von der Technik faszinierte Pioniere, verspielte „Frechdachse“ („scamps“), die niemanden schädigen wollen, Forscher, die in neue Bereiche vordringen wollen und Spieler, die Hacking insgesamt als ein Spiel betrachten (Kempa, 2006). Warren und Leitch (2009) haben sog. „Hacker-tagger“ identifiziert, die auf gehackten Websites sog. „tags“, also Markierungen hinterlassen, die – wie die „tags“ in der Graffiti-Kultur – die Urheber ausweisen, um Anerkennung in der Szene zu finden. Größere Schäden müssen dabei nicht angerichtet werden (Loper, 2009).

Nachfolgend seien Tätertypen im Bereich Identitätsdiebstahl und Softwarepiraterie erläutert. In beiden Fällen ist lediglich ein Subset der Täter der Cybercrime im engeren Sinne zuzurechnen.

5.3.1 Identitätsdiebe

Das Thema Identitätsdiebstahl wird in dieser Arbeit nicht detailliert behandelt, handelt es sich bei der Gewinnung persönlicher Daten doch nur dann um Cybercrime i.e.S., wenn die Daten durch das Kompromittieren der Computer oder Netzwerke von Unternehmen oder Behörden erlangt wurden. Viele Arten der Gewinnung erfolgen allerdings in eher traditioneller Art und Weise, beispielsweise mittels Betrug über das Internet.

Newman und McNally (2005) sehen eine für Betrüger und Wirtschaftskriminelle entwickelte Tätertypologie auch für Identitätsdiebe als nutzbar an, handelt es sich doch ihrer Auffassung nach um opportunistische Täter. Basierend auf einer Arbeit von Weisburd et al (2001) zur Betrugskriminalität unterscheiden sie daher folgende Formen des Identitätsdiebs:

(1) Niederfrequente Täter, die sich wiederum unterscheiden lassen in

a) Täter, die mit Kriminalität auf eine beliebige, von ihnen empfundene persönliche Krise reagieren („crisis responders“) (z. B. Eltern, die im Namen ihres Kindes ein Konto eröffnen, weil diese nicht mehr kreditwürdig sind).

b) Gelegenheitstäter („opportunity takers“), die einer sich ihnen öffnenden Tatgelegenheit nachgeben (z. B. der Kassierer, der die liegen gelassene Kreditkarte eines Kunden an sich nimmt).

(2) Hochfrequente Täter, die sich unterscheiden lassen in

a) Gelegenheitssucher („opportunity seeker“), die nicht allein nach Gelegenheiten zur Begehung von Kriminalität suchen, sondern Kriminalität fördernde Gelegenheiten selber schaffen und

b) stereotype Kriminelle („stereotypical criminals“) als die hochfrequentesten Täter, die

nicht nur kriminalitätsbezogen vorbelastet sind, sondern oftmals auch schon eine schwere Kindheit hatten, Drogen missbrauchen oder andere Probleme haben. Diese Täterkategorie ist in allen Bereichen des Identitätsdiebstahls zu finden, wird insbesondere jedoch als relevant für OK-Aktivitäten gesehen.

Newman und McNally (2005) weisen darauf hin, dass nicht allein die o. g. Tätertypen zum Problem beitragen, sondern auch die Wirtschaft und andere Organisationen, wenn sie bspw. „credit header" mit den persönlichen Daten des Kunden verkaufen. Dazu zählen auch Websites, die Bankverbindungen oder Sozialversicherungsnummern weiterverkaufen.

Morris (2010) unterscheidet vier Fertigkeitsniveaus von Identitätsdieben, wobei nur die beiden höchsten („sophisticated" und „highly sophisticated identity theft") einen direkten Bezug zur Cybercrime i. e. S. aufweisen. Indikatoren für erstgenannte Kategorie, die für etwa 25% der Fälle steht, sind beispielsweise die Einbeziehung von Computertechnologie bzw. der digitale Identitätsdiebstahl, während sich letztgenannte Kategorie, die nur für 6% der Fälle steht, insbesondere durch das arbeitsteilige Zusammenwirken bzw. einen hohen Organisationsgrad auf Täterseite auszeichnet (ebd.).

5.3.2 Raubkopierer bzw. Softwarepiraten

Sprachlich ein wenig ungenau unterscheiden Krömer und Sen (2011) drei Typen von Raubkopierern, d. h. Tätertypen, die Software, Musik, Filme oder auch Bücher gegen geltendes Recht vervielfältigen. Wie die nachfolgenden Ausführungen zeigen, meinen sie weniger Raubkopierertypen als vielmehr Szenen unterschiedlich qualifizierter Hacker bzw. Täter.

(1) Release Szene (auch Warez-Szene genannt):

Die Release Szene ist eine nach außen streng abgeschlossene Vereinigung von Raubkopierern, die aus unterschiedlichen Gruppen, den Release-Groups, gebildet wird. Unter selbstgewählten Namen firmierend, versuchen diese Gruppen in einer Art sportlichem Wettkampf, den Kopierschutz einer Software, eines Films oder eines Musikalbums auszuhebeln und als erste Gruppe eine Kopie eines solchen Originals zu erstellen, um diese als sog. „Release" zu verbreiten. Diese Tätigkeit findet weitestgehend in den für Außenstehenden nicht zugänglichen Teilen des Internets unter Wahrung der Anonymität statt.

Release-Groups verfügen über eine klare, hierarchische Struktur (vom Leader bis zum einfachen Member). Als Syndikat aus Sicht des FBI hochorganisiert, haben einzelne Mitglieder feste Aufgabenbereiche und können sich in der Gruppe hocharbeiten. Neben dem „Cracker", der für das Überwinden des Kopierschutzes erforderlich ist, ist eine der wichtigsten Positionen der „Supplier", der möglichst frühzeitig ein vor der Veröffentlichung stehendes Original (Software, Musik, Film) im Original beschafft. Rückgrat einer jeden Guppe sind die sog. „Maulwürfe" bei den Entwicklern, Vertriebsfirmen oder in Presswerken, die andere mit Informationen bzw. Daten versorgen.

Die Release-Szene ist für Krömer und Sen (2011) im Ergebnis eine Gemeinschaft des Raubkopierens, die sich durch klare Regeln und Wertvorstellungen, gemeinsame Verhaltensweisen, einen gemeinsamen Jargon und eine differenzierte interne Organisation auszeichnet. Sie ist diejenige Szene, die sich als einzige im Kern als Hacker-Szene qualifizieren lässt.

(2) FXP-Szene

Die FXP-Szene ist nach der Release-Szene die zweithöchste Stufe in der Piraten-Rangfolge. FXP-Szene stellt Raubkopien nicht selber her, sondern tauscht die aus der Release-Szene erhaltenen Kopien lediglich innerhalb ihrer eigenen Szene. Für die Speicherung der Kopien auf FTP-Servern werden auch keine eigenen, sondern fremde Computernetzwerke genutzt.

Szene-Mitglieder, die Zugang zu raubkopierten Filmen, Musikstücken oder Softwareprogrammen erhalten, verpflichten sich im Gegenzug, sich aktiv an der Verbreitung des Materials zu beteiligen. Das bedeutet in der Praxis, das Internet nach ungesicherten Servern zu durchsuchen, diese zu hacken und versteckten Speicherplatz darauf einzurichten, so dass die eigentlich Berechtigten Raubkopien nicht bemerken. Aus diesem Grunde werden Server bevorzugt, die hohe Datenumsätze haben, wie bspw. Rechner von Hochschulen oder größeren Unternehmen.

Ähnlich der Release-Szene hat sich eine Arbeitsteilung entwickelt: „Scanner“ durchsuchen das Internet nach geeigneten FTP-Servern und übermitteln Funde an die für das Hacken dieser Server zuständigen Mitglieder. Da das Hacken in diesem Feld häufig nur das Abarbeiten von Anleitungen bedeutet, handelt es sich bei der Tätigkeit nach Meinung vieler Hacker um kein richtiges Hacking. Zudem widerspricht die Tätigkeit den Grundsätzen des „ethischen Hackens“. Hacker in der FXP-Szene werden daher zumeist als „Haxxor“ bezeichnet. Sobald Zugang zu Rechnern besteht, ist es Aufgabe der „Filler“, die Rechner mit Raubkopien zu füllen (ebd.).

(3) Filesharing-Nutzer

Diese Gruppe beinhaltet die Endnutzer der Raubkopien, die, ohne selber über besonderes technisches Wissen verfügen zu müssen, auf die Daten mittels sog. Filesharing-Programme zugreifen. Heute gibt es eine Vielzahl derartiger Programme, die die Nutzer lediglich auf ihren Computer aufspielen müssen, um auf illegale Daten zugreifen zu können. Zu den bekanntesten gehören LimeWire und BitTorrent, über die vornehmlich urheberrechtlich geschützte Daten ohne Zustimmung der Rechteinhaber verbreitet werden (ebd.).

5.4 Arbeitsteiliges Vorgehen und „underground economy“

Aus Sicht von IT-Sicherheitsunternehmen wie auch der Polizei ist das Bild isoliert agierender Hacker überholt (Chabinsky, 2010; Fritsche, 2014; Kaspersky und Interpol, 2014). Heute ist Cybercrime in weiten Teilen einem unternehmerischen Geschäftsmodell vergleichbar, das sich durch eine komplexe, hoch organisierte Hierarchie mit einer Art Geschäftsführung, Ingenieuren, Fußvolk („infantry“) und angeheuerten Geldkurieren („money mules“) auszeichnet. Die oben beschriebene organisierte Raubkopiererszene steht beispielhaft dafür.

Von außen betrachtet unterscheidet sich die Organisation arbeitsteiligen Hackens kaum von anderen Geschäftsmodellen, in denen Mitarbeitern spezifische, ausgewiesene Funktionen zugeschrieben sind und der Auftrag insbesondere lautet, Geld zu verdienen. Die Spannbreite an Arbeitsergebnissen ist groß und reicht von Beratungsdiensten über Dienstleistungen jeder Art bis hin zu einer Unmenge an Produkt-Varianten bzw. hier den Programmen (Fortinet, 2013).

Nach Aussagen des FBI (Chabinsky, 2010) sind bei Cyberkriminellen im Zuge der Professionalisierung immer ausgefeiltere Wege der Kommunikation wie auch der Arbeitsorganisation feststellbar. In vielen Fällen der jüngeren Zeit zeigten sich geschäftsmäßige Arbeitsstrukturen mit einer außergewöhnlichen Logistik. Die Organisationen bestehen typischerweise aus kleinen Gruppen zuverlässiger Mitglieder mit unterschiedlichen Fertigkeiten, die einer möglichst effizienten Zusammenarbeit dienen. Eingebunden sind ferner Auftragnehmer, die ohne über ein vollständiges Bild der kriminellen Geschäfte zu verfügen und ohne Beteiligung an privaten Chatkanälen doch wichtige Teilaufgaben bspw. der Programmierung, der technischen Wartung, des Geldtransports oder ähnliches erledigen. Diese Form der Arbeitsteilung erlaubt es den unterschiedlichen Rollenträgern in ihrem jeweiligen Bereich Reputation zu erwerben und feste wie einträgliche Kundenbeziehungen aufzubauen, ohne selber ein kriminelles Unternehmen gründen zu müssen.

Das FBI (Chabinsky, 2010) hat zehn mögliche Spezialisierungen bzw. Arbeitsteilungen festgestellt, die sich in typischen Cybercrimedelikten wiederfinden:

1. Kodierer („coders“) bzw. Programmierer („programmers“) erstellen die zur Tatbegehung notwendige Malware, Exploits etc.
2. Verbreiter („distributors“) oder Verkäufer („vendors“) handeln bzw. verkaufen gestohlene Daten und bürgen für die Güter bzw. Leistungen, die durch andere Bereiche zur Verfügung gestellt werden.
3. Techniker („techies“) sind zuständig für die Unterhaltung der technischen Infrastruktur (wie Server, unverwundbare ISPs, Verschlüsselung) und verfügen häufig über Programmierkenntnisse.
4. Hacker suchen nach Schwachstellen in Anwendungen, Systemen und Netzwerken mit dem Ziel, Administratorenrechte oder Zugang zur Buchhaltung zu bekommen.
5. Betrugsspezialisten entwickeln Maßnahmen des Social Engineering und setzen diese ein, einschließlich Phishing, Spamming und Domain-Missbrauchs („domain squatting“).
6. „Hosts“ stellen sichere Inhaltsserver und Seiten zur Verfügung; oftmals über hochentwickelte Botnetze und Proxy-Netzwerke.
7. Einlöser („casher“) kontrollieren sog. „Drop-Accounts“ und verkaufen deren Inhalte an andere Kriminelle; sie managen zudem Zahlungskuriere, sog. „money mules“.
8. „Money mules“ transportieren bzw. transferieren die kriminellen Erlöse zu Dritten bzw. sicheren Orten.
9. Bankkassierer helfen bei dem Transfer und der Wäsche von illegalen Einnahmen durch digitale Währungsdienste und zwischen verschiedenen nationalen Währungen.

10. Führungskräfte der Organisation, die oftmals über überhaupt keine technischen Kenntnisse verfügen; sie entscheiden u. a. über Ziele, Ressourceneinsatz und Verwendung krimineller Erlöse.

Die hier aufgeführten Spezialisierungen sind lediglich beispielhaft zu verstehen, reflektieren Arbeitsteilungen doch auch immer nicht nur Geschäftsmodelle, sondern auch immer die jeweiligen Besonderheiten von Personennetzwerken und ihren Hauptakteuren. Aus den Ergebnissen einer Analyse englisch- und russischsprachiger Online-Schwarzmärkte für gestohlene Daten berichten Hutchings und Holt (2015) beispielsweise eine arbeitsteilige Struktur u. a. mit den Funktionen Verkäufer, Käufer, Lieferant, Moderator (zuständig für die Aufrechterhaltung der Ordnung und Durchsetzung von Regeln auf einem Marktplatz), Administrator (zuständig für die Organisation der Plattform und das Hosten von Foren) sowie Lehrer (zuständig für die Erstellung von Anleitungen etc.).

Im Zusammenhang mit der aus über 50 Personen bestehenden GameOver ZeuS-Gruppe berichtet Sandee (2015) von einem aus zwei Personen bestehenden Kern-Team, einem technischen Unterstützungsteam und einer Anzahl präferierter Lieferanten. Eng mit dem Kernteam verbunden war eine Anzahl von Nutzern, deren Aufgabe die Behebung von Fehlern und die Einführung bestimmter Funktionen war. Weitere Akteure waren für die Rekrutierung von Konten zum Herausziehen der illegalen Gewinne zuständig. In organisatorischer Hinsicht kann man die GameOver ZeuS-Gruppe der Organisationsform „hubs“ zuordnen, wie sie in Kapitel 5.5 beschrieben ist.

In einer Analyse zu Bedrohungen mobiler Endgeräte beschränken sich Kaspersky und Interpol (2014: 9) auf eine lediglich dreistufige, pyramidenförmige Akteurskategorisierung: Grundlegende Kategorien sind demnach die Infektoren an der Basis, die Analysten und die Investoren. Die Rolle der Infektoren wird beschrieben als die massenhafte Ausbeutung von Geräten bzw. die massenhafte Datengewinnung aus Geräten, ohne im Vorfeld nach Datenkategorien zu differenzieren. Motto ist: Je mehr Daten, desto besser. Rolle des Analysten ist die Auswertung der gewonnenen Daten im Hinblick auf eine Monetarisierung, d. h. die geldwerte Verwertung im Untergrund, die Erpressung von Geschädigten oder die Nutzung der auf dem Gerät gespeicherten Information zu Investition auf Märkten zum Beispiel in Form des Insider-Handels. Aufgabe des Investors an der Spitze der Pyramide ist die finanzielle Ausstattung des kriminellen Unternehmens. Dafür erhält der Investor den Löwenanteil des erwirtschafteten Profits.

Beispielhaft für die zwischenzeitig erreichte Arbeitsteilung ist das nebulöse Russian Business Network, das eine komplette Infrastruktur zur Begehung cyberkrimineller Handlungen (Phishing, Hosting von Malware, Glücksspiel oder Kinderpornographie) bereitstellt (Bizeul, 2007). Ähnliche Angebote existieren mittlerweile auch in China (Gu, 2013) oder Brasilien (Mercês, 2014); letzteres einschließlich Fortbildungen u. a. in Form von „how-to“-Videos.

Die Organisationsstruktur, die „Crime as a Service“ (CaaS) möglich macht, beschreibt der IT-Sicherheitsdienstleister Fortinet (2013) wie folgt: Wie in jedem legalen Unternehmen setzt die „Chefetage“ bzw. die Geschäftsführung („Executive Suite“) das Geschäftsmodell und die Infrastruktur auf. Sie trifft die wesentlichen Unternehmensentscheidungen, beaufsichtigt das operative Geschäft und stellt sicher, dass alles möglichst reibungslos funktioniert. Die Zusammenarbeit mit Partnern sowie strategische Planung bspw. hinsichtlich der Ausweitung

des Geschäfts gehört ebenfalls zu ihren Aufgaben.
Aufgabe des mittleren Managements ist es, so viele Rechner wie möglich zu infizieren, was diese Kräfte entweder selber erledigen oder mittels Personalvermittler („recruiter“) angeworbener Mitarbeiter, dem Fußvolk („Infantry“). Dieses steht am Ende der Befehlskette und ist für die Umsetzung der Angriffe verantwortlich. Häufig durch Anzeigen angeworbene Geldkuriere („money mules“) stellen abschließend das Waschen der kriminellen Gewinne sicher. Die Geldbewegungen erfolgen regelmäßig durch anonyme Transferdienste, wie sie bspw. durch Western Union, Liberty Reserve, U Kash oder WebMoney angeboten werden.
Speziell zur Anwerbung von Kräften werden Web-Portale eingerichtet. Viele dieser Portale kommen aus Russland („Partnerkas”) und sind nur auf Einladung zugänglich. Es gibt allerdings auch offene Portale.
Um das Fußvolk mit den richtigen Werkzeugen auszustatten, kümmert sich das mittlere Management um die Entwicklung der Werkzeuge zur Infektion von Systemen. Diese können bspw. gefälschte Antivirenprogramme, Erpressungsprogramme („ransomware“) oder auch Botnets umfassen.
Vergleichbar dem legalen Wirtschaftsleben reicht es in dem Geschäftsmodell CaaS nicht aus, über ein gutes Produkt zu verfügen; erforderlich sind sowohl Produkt- als auch Unternehmenswerbung; letzteres zugleich zur Gewinnung von Personal. Entsprechende Anzeigen können in online-Arbeitsbörsen, in Hacking-Foren sowie auf IRC-Chat-Kanälen bspw. mit Überschriften wie „Want to earn money online?” erscheinen.
Typische kriminelle Dienstleistungen („crime services“) sind laut Fortinet (2013) Beratungsdienste wie die Einrichtung eines Botnetzes, Infektions- bzw. Verbreitungsdienste, Upgrade-Module für sog. Crimeware oder auch Passwort-Cracker für die Cloud.
Die Backend-Bereiche der Untergrund-Wirtschaft („underground economy“) sind variantenreich und komplex. Je nach geschäftlicher Anforderung der Organisation werden z. B. private Bot-Netze, gefälschte Antivirensoftware oder Exploit-Codes erstellt. Vor dem Einsatz durchlaufen Codes einen Qualitätssicherungsprozess um einwandfreien Funktionieren möglichst ohne Detektion zu gewährleisten.
Für den Erfolg von Cyberkriminellen sind Hosting-Provider aus Sicht von Fortinet (2013) ein kritischer Faktor. Sie stellen den Speicherraum für die für Angriffe benötigten Inhalte (wie Exploit-Code, Malware und gestohlene Daten). Dabei kann es sich um offizielle Provider oder Dienste handeln, die kompromittierte Systeme bereitstellen. Hosting-Provider finden sich zum Teil in international sicheren Häfen wie Russland oder China, sind allerdings auch in Ländern wie den USA anzutreffen. Sie ignorieren zum Teil wissentlich, dass illegale Inhalte auf ihren Servern gespeichert sind. Häufig finden sich allerdings auch kompromittierte Server, die ohne Wissen der Provider genutzt werden.

Cyberkriminelle richten permanent neue Domains ein, während alte geschlossen werden, um eine Aufdeckung bzw. Erkennung zu verhindern. Das Schließen maliziöser Webseiten und Öffnen neuer ist vergleichbar dem Rennen von Hase und Igel, nur dass hier auf eine geschlossene Domain zwei neue eröffnet werden. Automatisierte Registrierungsprozesse und die täterseitige Nutzung gestohlener Kreditkarten helfen dabei (ebd.)

5.5 Cybercrime und Organisierte Kriminalität

Das begrenzte Wissen von Forschung, Praxis und Politik über Täter im Bereich Cybercrime bezieht sich ebenfalls auf die Strukturen krimineller Gruppen bzw. Netzwerke, die im Cyberraum operieren (McGuire und Dowling, 2013a). Auch wenn etwa 25% der Befragten im britischen Commercial Victimisation Survey 2012 davon ausgingen, dass ihre jüngsten Vorfälle von Online-Kriminalität durch eine organisierte Gruppe Krimineller und nicht von Einzeltätern begangen wurde, liegen dafür keine unabhängigen Bestätigungen vor (ebd.).

Auf der Basis eines Review von McGuire (2012; vgl. BAE Detica, 2012) könnte bis zu 80% der Cyberkriminalität Ergebnis irgendeiner Art organisierter Aktivität sein („some form of organized activity"), wie sie im Kapitel 5.4 beschrieben ist. Das bedeutet jedoch nicht, dass diese Gruppen die Form traditioneller, hierarchisch organisierter Gruppen haben oder dass diese Gruppen ausschließlich digitale Kriminalität begehen müssen.

Einer dreistufigen Typisierung von Organisierter Kriminalität folgend (Choo und Smith, 2008) lässt sich zwischen traditionellen, hierarchisch organisierten Gruppen der Organisierten Kriminalität (Typ 1), gleichgesinnten Personen, die sich lediglich aus dem Netz kennen und dennoch in organisierter Form zur Erreichung eines gemeinsamen Zieles zusammenarbeiten (Typ 2) und politisch motivierten OK-Gruppen (Typ 3) unterscheiden.
Gruppen des Typs 1 zeichnen sich dadurch aus, den Wert neuer Technologien für die Begehung von Straftaten (z. B. Erpressung, Betrug, Verbreitung illegaler Inhalte) und die Geldwäsche erkannt zu haben (vgl. dazu Tabelle 5). Globale Gruppen der Organisierten Kriminalität wie die asiatischen Triaden oder die japanischen Yakuza können demnach direkt mit Cyberstraftaten (wie z. B. Softwarepiraterie, Kreditkartenfälschungen, Betrug) verlinkt werden (Broadhurst et al., 2013; Choo und Smith, 2008).
OK-Gruppen vom Typ 2 profitieren davon, dass es das Internet erheblich einfacher macht, auch über größere Entfernungen hinweg Aktivitäten zu planen. Selbst wenn die Ziele von Typ 2-Strukturen zumeist finanzieller Natur sind, ist u. a. auch die Produktion und Verbreitung von kinderpornographischem Material möglich (online-Pädophilenringe). Von ihrer Organisation her unterscheiden sich diese Gruppen in signifikanter Form dadurch vom Typ 1, dass die Zusammenarbeit auch in zeitlicher Form dadurch limitiert ist, dass lediglich eine bestimmte Aufgabe in Projektorganisation gemeinsam abgearbeitet wird und man sich danach wieder trennt (vgl. auch Broadhurst et al., 2014). Die Struktur ist eher lose und flexibel sowie transnational; die Zahl an Gruppenmitgliedern eher geringer. Das hängt auch damit zusammen, dass physische Kraft im Gegensatz zu traditionellen Gruppen nicht in Form vieler Personen beispielsweise zur Ausübung von Gewalt, sondern in Form potenter Software benötigt wird (Choo und Smith, 2008). Individuen in Gruppe 2-Typen haben wahrscheinlich eine höhere technologische Potenz (ebd.).
Politisch motivierte OK-Gruppen vom (Typ 3) werden erst seit den Anschlägen 2001 diskutiert; vorher galten Terrorismus und Organisierte Kriminalität gemeinhin als getrennte Größen. In jüngerer Zeit wird eine Konvergenz zwischen beiden wahrgenommen, für die beispielhaft die Geldwäscheaktivitäten von Al Quaida stehen (Choo und Smith, 2008). Straftaten, die gemeinhin OK-Gruppen zugeschrieben wurden, wie z. B. online-Betrugsmaschen, Identitätsdiebstähle, Einreisestraftaten oder Warenfälschungen gelten nun auch als Vorbereitungstaten, die von terroristischen Gruppen bspw. zur Geldbeschaffung eingesetzt werden. Darüber hinaus können sich kriminelle Organisationen mit der Zeit auch ideologisieren. In Südasien wurden z. B. ideologische oder religiöse Prägungen übernommen, die die Gruppen motivieren und nicht lediglich ihre Taten verdecken sollen. Lai (2005)

berichtet zudem von terroristischen Gruppen, die sich zur Versorgung mit Waffen und Munition auf OK-Gruppen verlassen und diese als Gegenleistung u. a. im Gebrauch von Waffen und Sprengstoff ausbilden (Choo und Smith, 2008).

Tabelle 5: Übertragung der Tätigkeitsbereiche traditioneller OK in die Online-Welt (BAE-Detica; 2012)

Traditioneller Indikator	**Onlineparallelität**
1) Erpressungstechniken	- Androhen der Schließung von IT-Systemen durch Malware-Attacken - Nutzung kompromittierter Browserdaten, die mittels Key-logging gewonnen wurden, für Erpressungen
2) Kontrolle von Glücksspiel	- Entwicklung von neuen Offshore-Einkommensströmen - Erpressung von Glücksspiel-Websites
3) Kontrolle von Drogenmärkten	- Schaffung von Internetzugängen zu verschreibungspflichtigen Drogen - Verkäufe von illegalen Drogen - Entwicklung von Drogenmärkten für gefälschte Ware (Viagra etc.)
4) Geldwäsche	- Wäsche digitaler Einnahmen - Globale Geldkurier-Systeme („money mules“)
5) Fälschungskriminalität	- Organisierte Banden, die DVDs kopieren - Organisierter Diebstahl geistigen Eigentums
6) Sex und Prostitution	- Bildung von Imperien für Online-Pornographie - Verbindungen zwischen Eskort-Angeboten, Menschenhandel und organisierten Banden
7) Gewaltkriminalität	- Angriffe auf Carding-Foren zur Übernahme von Rivalen - Bereitschaft zur Nutzung von Gewalt zur Gewinnung von Identifikationsdaten oder um digitale Währungen zu erbeuten

Ob man kriminelle Aktivitäten auch definitorisch immer eindeutig der organisierten Kriminalität zurechnen kann, ist aus Sicht von Lusthaus (2013) zweifelhaft. Wie bereits angedeutet liegen deutliche Hinweise dahingehend vor, dass „organisierte“ Cyberkriminelle eher in lockeren Netzwerken als in formalen Organisationen zusammenwirken und dabei globale online-Marktplätze zum Kauf und Verkauf von Waren und Dienstleistungen nutzen. Diese Gruppen arbeiten zwar gemäß einer Organisationsstruktur; die Teilnehmer sind allerdings anders als bei traditionellen Gruppen der OK nicht durch dieselbe Form von Hierarchie und Führung gebunden, sondern agieren projektbezogen locker miteinander verbunden für kürzere, begrenzte Zeiträume anstelle einer dauerhaften Zusammenarbeit

(Broadhurst et al., 2014; Choo und Smith, 2008; Décary-Hétu und Dupont, 2012; Europol, 2015; Holt, 2013; Hutchings, 2014; Lusthaus, 2013).

Broadhurst et al. (2014) berichten unter Bezugnahme auf das von McGuire (2012) durchgeführte Review, dass dort die Hälfte der Cybercrime-Gruppierungen aus sechs oder mehr Personen, ein Viertel der Gruppen sogar aus mehr als zehn Personen bestand. Ein Viertel der Cybercrime-Gruppen war weniger als sechs Monate aktiv. Weder die Größe der Gruppe noch die Dauer der Aktivität lassen jedoch Aussagen zu Ausmaß und Schwere der begangenen Straftaten zu.

Hinsichtlich der Organisation und Kommunikation in den Gruppen selber schlägt McGuire (2012) eine sechsstufige Typisierung mit drei Hauptgruppen und jeweils zwei Untergruppen vor. Diese Grundmuster sollten allerdings nicht statisch interpretiert werden (Broadhurst et al., 2014).

Typ 1-Gruppen operieren danach im Wesentlichen online und können unterschieden werden in Schwärme („swarms“) und Drehscheiben bzw. Netzknoten („hubs“)

(1) Schwärme teilen viele der Merkmale eines Netzwerkes und können beschrieben werden als „disorganisierte, führungslose Organisationen mit einem gemeinsamen Zweck“. Typische Schwärme verfügen über minimale Führungsstrukturen und operieren in viraler Form. Beispielhaft dafür sind die Aktivitäten früher hacktivistischer Gruppen. Schwärme scheinen am ehesten in Ideologie getriebenen Aktivitäten wie Hass-Kriminalität und dem politischen Widerstand zu finden zu sein. Beispielhaft dafür ist Anonymous (Robertz und Rüdiger, 2012; Olson, 2012).

(2) Drehscheiben bzw. Netzknoten („hubs“) verfügen anders als Schwärme über einen gewissen Organisationsgrad und eine Kerngruppe von Kriminellen (den „hub“), um die herum sich andere Täter gruppieren. Zu den diversen online-Aktivitäten zählen Pirateriedelikte, Phishing-Attacken, Botnetze o.a. die Verbreitung von Scareware. Märkte zur Verbreitung gestohlener Kreditkartendaten oder Rauschgift-Märkte wie SilkRoad lassen sich ebenfalls als „hub“ klassifizieren.

Typ 2-Gruppen kombinieren als Hybridkategorien online- und offline-Kriminalität und lassen sich unterteilen in „gebündelten Hybrid“ („clustered hybrids“) und „erweiterten Hybrid“ („extended hybrids“).

(3) Bei „gebündelten Hybriden“ geschieht die Kriminalität um eine kleine Gruppe von Individuen herum und konzentriert sich auf spezifische Aktivitäten oder Methoden. Durchaus ähnlich den „hubs“ wird allerdings nahtlos zwischen online- und offline-Kriminalität gewechselt. Eine typische Gruppierung skimmt Zahlungskarten, um diese dann für online-Käufe zu verwenden oder die Daten durch Carding-Netzwerke zu verkaufen.

(4) Gruppen im Bereich der „erweiterten Hybride“ operieren ähnlich den gebündelten Hybriden, sind jedoch viel weniger zentralisiert. Typischerweise umfassen sie viele Mitarbeiter und Untergruppen. Sie führen eine unterschiedliche kriminelle Aktivitäten aus, wobei immer ein bestimmtes Niveau an Koordination bleibt, das den Erfolg der

Operationen sicherstellen hilft.

Typ 3-Gruppen operieren hauptsächlich offline, nutzen allerdings Technologie zur Erleichterung ihrer Aktivitäten. Aus McGuires Sicht ist dieser OK-Gruppentyp zunehmend an der digitalen Kriminalität beteiligt. Er lässt sich weiter differenzieren in „Hierarchische Gruppen“ („hierarchies“) und „aggregierte Gruppen“ („aggregates“):

(5) „Hierarchische Gruppen“ lassen sich am besten beschreiben als traditionelle kriminelle Gruppierungen (z. B. die kriminellen Familien), die einen Teil ihrer Aktivitäten nun online ausführen. Beispiel ist die Mafia-Organisation, die ihre Prostitutionsaktivitäten nunmehr im Bereich pornografischer Websiten ausbauen. Andere Beispiele umfassen online-Spiele oder auch Erpressungen mit der Drohung, IT-Systeme lahmzulegen.

(6) „Aggregierte Gruppen“ sind nur lose organisiert und agieren temporär ohne klares Ziel. Digitale Technologien werden ad hoc für kriminelle Zwecke missbraucht. Beispiele sind die Nutzung von Mobiltelefonen zur Koordinierung von Unruhen wie bspw. in UK 2011 oder in Sydney 2012.

5.6 Phasenmodell der Hackerentwicklung

Fokussiert man allein auf das Fertigkeitsniveau von Hackern, erscheint eine pyramidenförmige Struktur von Hackertypen naheliegend (Holt et al., 2012; Holt und Kilger, 2012; McGuire und Dowling, 2013a), wie sie in Abbildung 1 dargestellt ist. An der Spitze befinden sich eine kleine Zahl kenntnisreicher Hacker, die über substanzielle Fähigkeiten in der Analyse von Schwachstellen, der Erstellung von Exploits und der Implementation neuer Programme verfügen, die für unterschiedlichste Angriffsformen genutzt werden können. Andere Forscher bezeichnen diese Hacker, von denen zugleich die größte Gefahr ausgeht, vom Typ her als „elite hacker“ oder „black/white/grey-hacker“ (Jordan und Taylor, 1998; Furnell, 2002). Nach Aussage des ehemaligen Leiters des European Cyber-Crime Center bei Europol, Troels Oerting, ist weltweit von nur etwa 100 maßgeblichen Malware-Programmierern („cybercrime kingpins“) auszugehen (Heise, 2014).

Unterhalb dieser Ebene der hochqualifizierten Hacker befindet sich eine Schicht angelernter („semi-skilled“) Akteure, die die Fähigkeit besitzt, unterschiedlichste Hacking-Tools und Exploits sowohl zu erkennen als auch anzuwenden, auch wenn ihnen das technische Verständnis oder auch nur das Interesse fehlt, diese Tools selber zu entwickeln. Im Ergebnis nutzen sie die Tools anderer für eigene Cyber-Angriffe. Diese Gruppe von Hackern hat mit dem Aufkommen von Märkten gestohlener Daten in den letzten Jahren erheblich an Bedeutung gewonnen.

Der Boden der Pyramide ist mit Akteuren bevölkert, die über ein sehr geringes Fähigkeitsniveau verfügen bzw. als ungelernt qualifiziert werden. Hier finden sich laut McGuire und Dowling (2013a) die „skript kiddies“, die in ihrem Handeln gänzlich von höher qualifizierten Hackern abhängig sind. Holt und Kilger (2012) weisen darauf hin, dass auch diese Gruppe Schäden verursachen könne, in dem sie aufgrund ihres Interesses zu hacken selber Angriffsflächen für andere Hacker bilden können. Der Download von Schadsoftware

durch „script-kiddies“ kann z. B. durch qualifizierte Hacker ausgenutzt werden, um deren Computer zu infizieren und für eigene Zwecke zu missbrauchen. Zugleich lassen sich diese infizierten Computer als Frühwarnsysteme vor Aktionen der Strafverfolgungsbehörden nutzen, sobald gegen „script-kiddies“ vorgegangen wird. Mit der Etablierung von online-Schwarzmärkten haben ungelernte Täter noch in anderer Hinsicht an Bedeutung gewonnen. So können bspw. Hacker aus dem Mittelbau der Hackerpyramide ihre Infrastruktur an andere verpachten, um DDoS-Attacken durchzuführen oder Spam zu verbreiten (ebd.). Zugleich lassen sich Ungelernte nutzen, um in Geflechten der Cybercrime eher traditionelle Tätigkeiten wahrzunehmen wie z. B. das sog. Auscashen krimineller Gewinne.

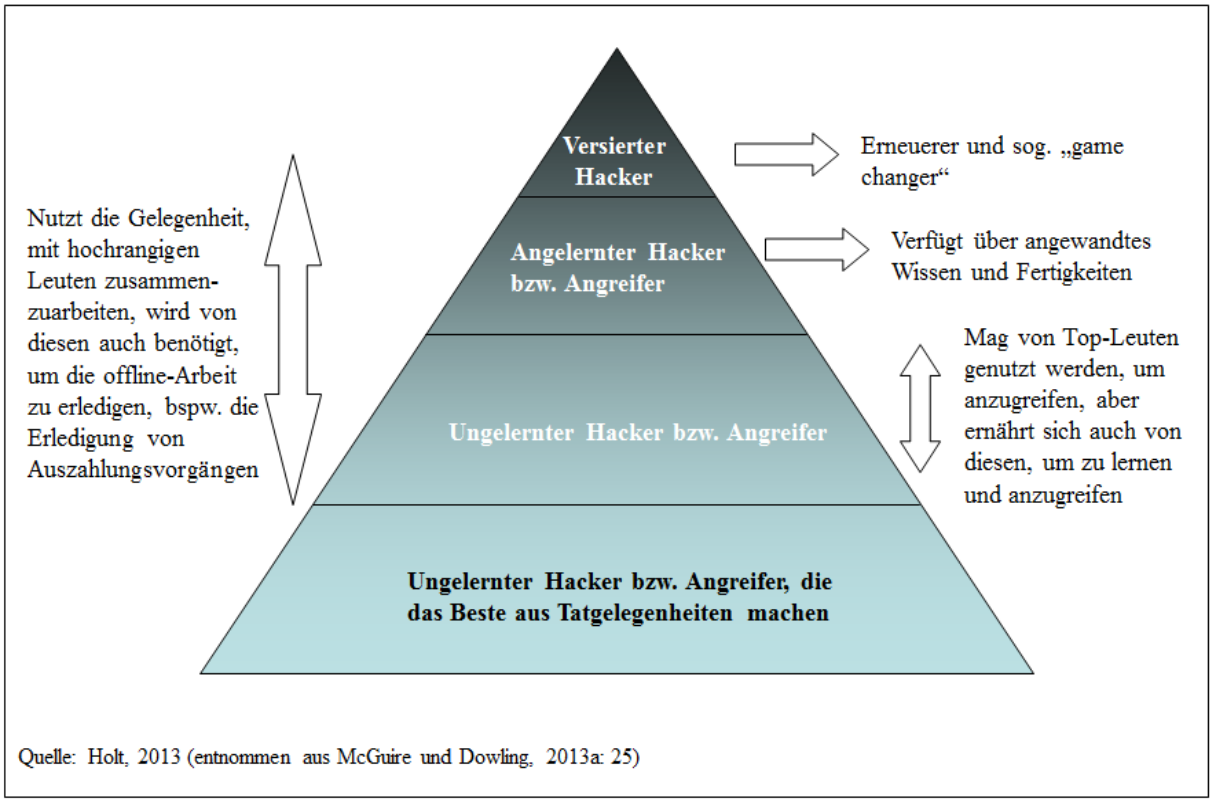

Abbildung 1: Fähigkeitspyramide der Cyber-Angreifer

Interessanterweise nutzen McGuire und Dowling (2013a) in ihrer pyramidenförmigen Strukturierung von Hackertypen (Abbildung 1), die auf Holt (2013) zurückgeht, nicht die üblichen Typenbezeichnungen für Hacker, was als ein Indiz dafür interpretiert werden könnte, dass Hackertypen nur schlecht voneinander abgrenzbar sind. Hacker lassen sich auch nicht immer eindeutig bestimmten Kategorien zuordnen, betrachtet man beispielsweise das Modell von Rogers (2000; vgl. Tabelle 1), auf das in der Literatur gerne Bezug genommen wird. In Kapitel 5.1 war bereits darauf hingewiesen worden, dass Typenbildungen regelmäßig nicht nur das Fertigkeitsniveau, sondern auch Motivlagen von Hackern abbilden. Die Ausführungen von Chiesa et al. (2009) zur Kategorie der „script-kiddies“ in Kapitel 5.1 sind ebenfalls ein Indiz dafür, dass mit bestimmten Begrifflichkeiten zwar gewisse Vorstellungen verbunden sind, bezogen auf „script-kiddies“ ist es die Abhängigkeit von Schadprogrammen qualifizierter Hacker, dass jedoch unabhängig davon das Fertigkeitsniveau dennoch eine gewisse Spannbreite aufweisen kann. Insoweit ist es nur schlüssig, dass Holt (2013) bzw.

McGuire und Dowling (2013a) in ihrer Fähigkeitspyramide nicht die üblichen Typenbezeichnungen oder Etikette für Hacker nutzen, sondern völlig neutral auf bestimmte Fertigkeitsniveaus referenzieren.

Unabhängig davon lädt das in Abbildung 1 vorgestellte System geradezu dazu ein, in einen karriere- bzw. entwicklungsspezifischen Fokus zu wechseln, wie ihn van Beveren (2001), Rennie und Shore (2007) und auch Picko und Hahn (2007: 32) vorgeschlagen haben.

Van Beverens (2001) „conceptual model" der Entwicklung vom „Tool kit/Newby" zum „Cyber Punk" oder „Old Guard" ist im Kern psychologisch basiert und nimmt insbesondere die von Csíkszentmihályi beschriebene Flow-Theorie auf (vgl. Kapitel 6.7). Darüber hinaus wird das Vorhandensein einer nicht weiter erläuterten Disposition bzw. „criminal tendency" angenommen, mittels derer die Entwicklung zu straffälligen Formen des Hackings („cyber punk") erklärt wird. Die in dem Modell verwendeten Tätertypen gehen auf eine frühe Hacker-Taxonomie von Rogers (vgl. Rogers, 2000) zurück. Der Beginn einer Karriere des Hackings wird bei den sog. „Tool kits/Newbies" bzw. „Script-kiddies" gesehen, die erfolgreich auf vorhandene Werkzeuge zurückgreifen können. Die weitere Entwicklung von Fertigkeiten hängt sowohl von den Werkzeugen als auch von den Herausforderungen in einer Online-Umgebung ab. Insbesondere Flow soll die stufenförmige Entwicklung bis hin zu einem (guten) „old-guard"-Hacker oder einem (böswilligen) „cyber-punk" erklären. Lediglich für die Innentäter („Internals") wird angenommen, dass sie unterschiedliche Stufen nicht durchlaufen müssen.

Rennie und Shore (2007) haben nachfolgend aufgezeigt, dass Flow-Erfahrungen nicht in der Lage sind, Cyberkriminalität in ihrer Vielfalt zu erklären. So unterscheiden sich doch beispielsweise Cyberterroristen, Hacktivisten, Penetrationstester und Cyberkrieger aus motivationaler Sicht zum Teil fundamental voneinander. Das von van Beveren (2001) vorgeschlagene Entwicklungsmodell haben sie nachfolgend angepasst und auch verfeinert. Aus Sicht von Rennie und Shore (2007) ist die Entwicklung vom „script-kiddie" zum „Cyber-Punk" nicht unvermeidlich. Tatsächlich kann sich der „script-kiddie" zum Cyberkriminellen („Cyber Criminal"), Hacktivist, „Cyber-Punk", Penetrationstester oder zu nichts von allem weiterentwickeln. Die Flowtheorie könne diese Entwicklung nur in Teilen beschreiben. In nachfolgender Abbildung 2, in der die Autoren van Beverens Modell fortschreiben, finden sich die Einflüsse von Flow auf der horizontalen Achse, während sich kriminelle Neigungen und Ideologie in eine vertikale Richtung und Karriere in die andere vertikale Richtung bewegen.

Was in dem Modell von Rennie und Shore (2007) allerdings völlig fehlt, sind die sog. Innentäter, wobei gerade dieser Begriff die Problematik von Etikettierungen deutlich macht, umfasst das Phänomen „Innentäter" doch ein ganzes Bündel an Motiven (z. B. Gelderwerb, Status, Rachsucht), an Absichtsgraden (von der fahrlässigen Pflichtmissachtung bis zur direkten Absicht) und an Fertigkeiten (sowohl bezüglich Hacking als auch in sozialer Hinsicht).

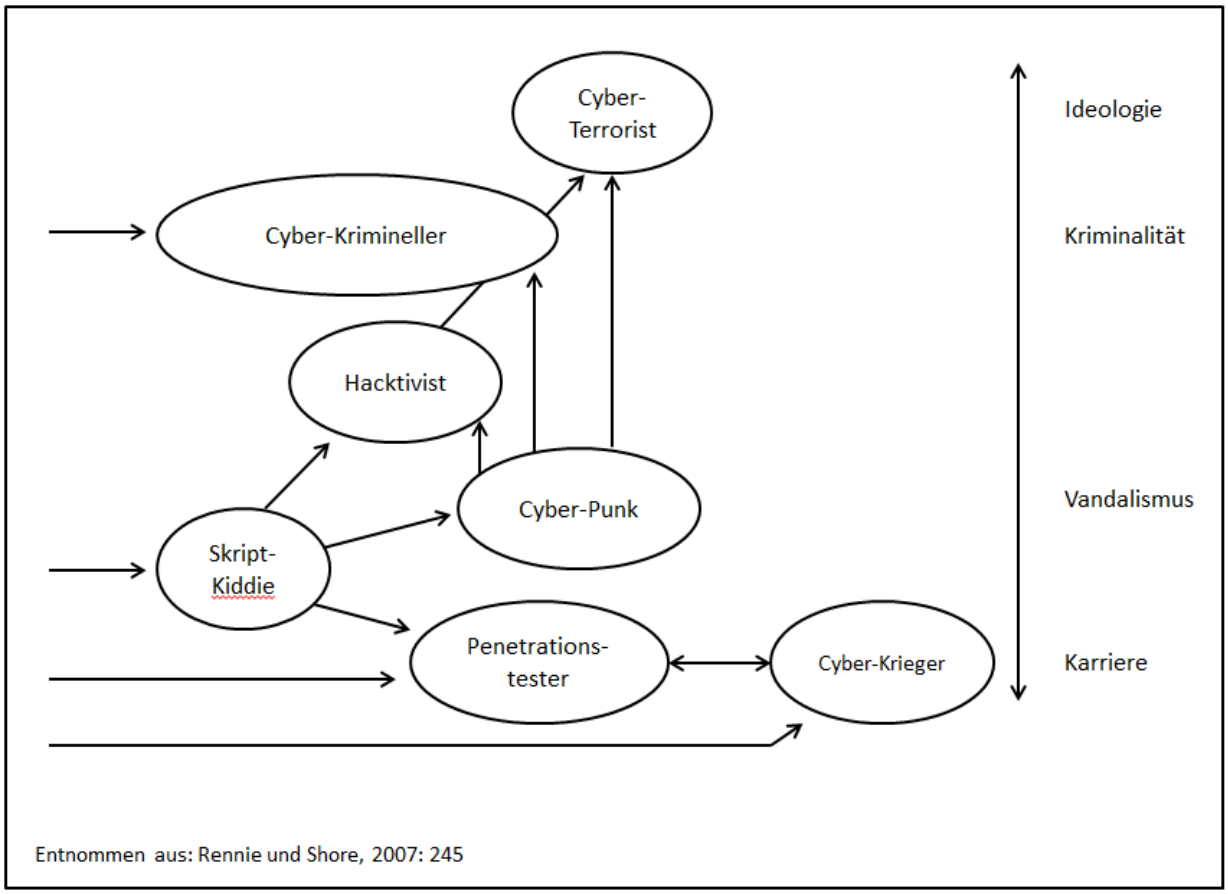

Abbildung 2: Modell der Hackerentwicklung

In der deutschsprachigen Literatur beschreiben Picko und Hahn (2007) die Entwicklung devianten Verhaltens im Bereich der Computerstraftaten im engeren Sinne in einem Dreiphasenmodell, das im Gegensatz zu dem Modell von Rennie und Shore (2007) erst spät eine moralisch-ethische Weiche enthält. Die Entwicklung devianten Verhaltens beginnt demnach beim ambitionierten User bzw. den hier besprochenen „script-kiddies“, die sich weitere Hackingfertigkeiten aneignen und am Ende zu „Hacktivisten“, „kommerziellen Hackern“ oder sog. „White-Hats“ werden. In der ersten Phase, die über mehrere Jahre gehen kann, muss sich der „angehende Hacker“ zunächst grundlegende Fertigkeiten zu Betriebssystemen, Anwenderprogrammen, Programmiersprachen, dem Internet und internetbasierten Kommunikationswegen aneignen. Er muss in dieser Phase ebenfalls lernen, Schadprogramme herunterzuladen und einzusetzen. Erleichtert wird dieser Prozess durch die in den letzten Jahren zunehmend erfolgte Bereitstellung benutzerfreundlichere Angriffswerkzeuge (Stichwort „crime as a service“). Den „script-kiddies“ muss dabei nicht zwingend bewusst sein, welche Schäden sie mit ihren scheinbar harmlosen Aktivitäten entfalten. Ggf. vertrauen sie in dieser Phase fälschlicherweise zudem darauf, dass ihr Handeln für Strafverfolgungsbehörden nicht rückverfolgbar ist (ebd.).
Auch wenn „script-kiddies“ in ihrer eigenen Subkultur wegen ihrer Erfolge anerkannt werden, gilt in der Szene der „echten Hacker“ doch nur derjenige etwas, der selber in der Lage ist, Schadprogramme („Exploits“) zu entwerfen bzw. auf unterschiedliche Anwendungsfälle hin anzupassen. Insofern wird sich eine Teilgruppe der „script-kiddies“ in einer zweiten Entwicklungsphase weitergehende Kenntnisse von Betriebssystemen und

Programmiersprachen erarbeiten und sich auch mit Expertensystemen befassen. „Echte Hackingerfolge“ bewirken für diese Personen nicht nur Anerkennung in der Hackerszene, sondern eröffnen über die Einladung zu spezifischen Kommunikationsplattformen auch einen besseren Zugang zu Experten. Das Unrechtsbewusstsein ist in dieser zweiten Phase aus Naivität oder aufgrund von szenetypischen Verdrängungs- bzw. Rechtfertigungsmechanismen wenig ausgeprägt. Hier dürften sowohl szenespezifische Feindbilder als auch die Grundsätze der Hackerethik eine Rolle spielen (ebd.).
Mit der Erreichung eines hohen Fertigkeitsniveaus sowie der Etablierung in der Szene verändert sich ggf. auch die Bedürfnisstruktur. Auf der Basis ethisch-moralisch geprägter Bedürfnisse sind sowohl die Hinwendung zu eher legalen Tätigkeiten (z. B. Lehre, Studium) als auch die Hinwendung zu illegalen Hacks möglich, letztere wenn es um die Verfolgung scheinbar höherwertiger politischer Ziele geht. Genauso möglich ist eine Hinwendung zur illegalen Bereicherung auf der Basis einer stark monetär geprägten Bedürfnisstruktur. In dieser dritten Phase werden Ziele bewusst ausgewählt; Angriffe erfolgen konzentriert und in einer Form, dass eine direkte Rückverfolgung durch die Polizei erheblich erschwert wird. Nicht ungewöhnlich ist es, wenn das hohe Expertenwissen dieser versierten Hacker sowohl beruflich, z. B. als IT-Administrator, als auch privat zur Begehung strafbarer Handlungen genutzt wird (ebd.). Die Bedürfnisstruktur ist in diesem Fall ambivalent; phänotypisch wäre dieser letzte Fall am ehesten den „grey hat“-Hackern zuzuordnen.

In den aufgezeigten Entwicklungsmodellen wird deutlich, dass Typenbezeichnungen für Hacker nicht nur Fertigkeitsniveaus und Motivlagen, sondern auch Karrieretypen abbilden. Dabei zeigt die ausgewertete Literatur allerdings auch, dass sich Begriffe nicht scharf voneinander trennen lassen. Beispiele dafür sind die sog. „script-kiddies“, cyberkriminelle Berufsverbrecher, die schon allein fertigkeitsbezogen eine gewisse Spanne abdecken können, sowie die sog. Innentäter, die phänomenologisch ein breites Spektrum an Motiven, Absichtsgraden und Fertigkeiten aufweisen können. Darüber hinaus gilt jedoch für jeden der in diesem Bericht bislang genannten Typen, dass deren Bezeichnung sozial konstruierte Etikette sind, die nicht auf einem einheitlichen und verlässlichen Kategoriensystem fußen.

5.7 Zwischenfazit

Vorliegende Literaturanalyse hatte die Typisierung unterschiedlicher Täterausprägungen zum Ziel, um auf dieser Basis möglichst spezifische Herangehensweise an die jeweilige Zielgruppe herausarbeiten zu können. Diese Zielformulierung erscheint auf der Basis der Literaturanalyse kaum noch haltbar. Zumindest für die geradlinige Ableitung bestimmter Interventionen aus einem eng eingegrenzten Tätertypus gibt es kaum Ansatzpunkte. Die Gründe dafür sind vielfältig.

In den letzten 25 Jahren sind Hacker vorrangig nach ihrem Fertigkeitsniveau, dem Zweck bzw. der Motivation ihres Handelns und in neuerer Zeit auch nach ihrer beruflichen Herkunft bzw. ihrem Auftraggeber typisiert worden. Regelmäßig fanden mehrere dieser Faktoren gleichzeitig Berücksichtigung, wie Tabelle 2 (Gesamtübersicht der bis zum Jahr 2000 publizierten Typisierungen) oder auch die Klassifizierungen von Chiesa et al. (2009) und des niederländischen National Cyber Security Centre (NCSC, 2014) exemplarisch zeigen.

Hinweise zur methodischen Herangehensweise an die Entwicklung von Tätertypisierungen im Bereich Hacking fanden sich in der Literatur keine. Das Objekt der Typisierung scheint so faszinierend zu sein, wie ja auch insbesondere frühe Fremd- und Selbstbilder von Hackern belegen, dass kein Raum mehr für Methodisches blieb. Eine wirkliche Analyse des Prozesses der Typenbildungen von Hackern war insofern im Rahmen dieser Literaturerhebung nicht möglich.

Alle genannten Typisierungssysteme sind sowohl Ergebnis von Selbst- als auch von Fremdzuschreibungen. Bei Selbstzuschreibungen wie den in dieser Arbeit berücksichtigten Befragungen, ist immer der Aspekt der sozialen Erwünschtheit zu berücksichtigen. Es ist zu vermuten, dass Hacker durch ihre Enkulturation in einer Hackercommunity bestimmten internalisierten Verhaltenserwartungen gerecht werden wollen. Darüber hinaus ist nicht auszuschließen, dass in einer Befragungssituation *ex post*-Rechtfertigungen *ex ante*-Motivationen überlagern.

Je differenzierter Typisierungen werden, ein gutes Beispiel ist die feingliedrige Differenzierung der Grundtypen „white hat“, „black hat“ und „grey hat“ in Kapitel 5.1, desto schwerer erscheint eine valide Zuordnung. Häufig scheint schon die grobe Unterscheidung von guten und bösen Hackern fast unmöglich zu sein. Aus polizeilicher Sicht könnte an dieser Stelle hinzugefügt werden, dass die Regeln des Strafgesetzbuches den „guten Hacker“ kaum zulassen. Frühestens im Rahmen der justiziellen Würdigung des Hackerhandelns bleibt Raum für derartige Differenzierungen.

Solange verlässliche und allgemeingültige Täterdifferenzierungen nicht möglich sind, besitzen die in diesem Bericht genutzten Etiketten für (vermeintlich) unterschiedliche Hackertypen für die Polizei kaum einen praktischen Mehrwert, was im Weiteren damit zusammenhängt, dass in den meisten Verfahren kaum oder allenfalls wenig Informationen zu Tatverdächtigen vorhanden sind. Sollen die in diesem Bericht genannten Typenbezeichnungen genutzt werden, dann erscheint dies allenfalls in einer ex post-Betrachtung möglich. Im Anschluss an Hacks erfolgende frühe Zuschreibungen zu Kategorien erscheinen allenfalls im Bereich der politisch motivierten Kriminalität sinnvoll, soweit denn Selbstbezichtigungen vorliegen. Betroffen wären hier die Kategorien der „Hacktivisten“ und der „Cyber-Terroristen“.

Aus präventiver Sicht am hilfreichsten ist ggf. noch die Arbeit von Rheinberg und Tramp (2006), die Personen untersucht haben, die ihre Rechner in der Freizeit ungewöhnlich intensiv nutzen und in einem induktiven Ansatz auf der Basis selbstberichteter Nutzungsweisen lediglich drei grobe Nutzertypen herausgearbeitet haben: Neben den zweckorientierten Nutzern sind dies die (eher guten) Hacker und die auf Schäden abzielenden Cracker. Hier könnten weitere Forschungsarbeiten sinnvoll sein, mittels derer sowohl Anreiz- als auch Abschreckungsaspekte von Hackern und Crackern deutlicher herausgearbeitet werden und nach Wegen gesucht wird, Cracker in Richtung positiver bzw. in der Gesellschaft akzeptierter Hackeraktivitäten zu bewegen.

Aus kriminalstrategischer Sicht hilfreich erscheinen auch die Arbeiten des niederländischen National Cyber Security Centre (NCSC 2012 – 2014), dessen Berichte Gefahrenquellen, deren Potenzial, Zielrichten etc. so zu beschreiben suchen, dass auf dieser Basis staatliche Planungsentscheidungen ermöglicht werden.

Darüber hinaus sei ebenfalls aus kriminalstrategischer Sicht angemerkt, dass es sich lohnen

könnte, den Fokus insbesondere auf die oberste Schicht qualifizierter Hacker, die sog. „elite hackers“, „black/white/grey-hackers“ oder auch „wizards“, zu richten, ließe sich mit deren Neutralisierung die Entwicklung von Malware ggf. nachhaltig stören.

Teil II – Kriminologische Erklärungen und Handlungsmöglichkeiten

Da sich aus der Typisierung von Hackern allein kaum differenzierte Handlungsansätze ableiten lassen, wie die bisherigen Ausführungen zeigen, soll in diesem Teil nun untersucht werden, inwieweit klassische und ggf. auch neuere Kriminalitätstheorien Täterhandeln, Motivationen und auch Rechtfertigungen der Handelnden erklären können. Die Arbeit basiert ebenfalls auf der in Kapitel 3 beschriebenen Literaturanalyse. Die nachfolgende Betrachtung verzichtet auf eine Differenzierung von Hackertypen; sie bezieht sich auf das Thema Hacking insgesamt.

Ziel dieser Analyse war letztlich auch die Gewinnung von Informationen zu möglichen Interventionen, mittels derer Hacking unterbunden oder zumindest eingeschränkt werden könnte. Diese Handlungsmöglichkeiten wurden nicht gesondert erhoben, sondern basieren ebenfalls auf den Ergebnissen der Literaturanalyse.

6 Kriminologische Erklärungen

Der nachfolgende Abschnitt beschränkt sich auf diejenigen Theorien, die in der Literatur im Cybercrime-Kontext eine Begründung bzw. Anwendung erfahren haben. Soweit Theorien ohne weitere Diskussion oder Anwendungsbeispiele bloß genannt wurden, wurden sie hier nicht berücksichtigt. Hinweise auf weitere, hier nicht diskutierte Ansätze finden sich u. a. bei Jaishankar (2008) und Wada et al. (2012).

Die Berücksichtigung des Themas „Flow“ in diesem Kapitel hängt damit zusammen, dass Flow-Erfahrungen häufig im Begründungszusammenhang mit dem Hacken genannt werden. Flow ist natürlich weder ein ausschließlich kriminologisches Thema, noch kann es bestimmte Aktivitäten alleinig erklären. Aus der Struktur des Berichts heraus erschien es jedoch am sinnvollsten, das Thema in diesem Kapitel aufzunehmen.

Bei retrospektiver Betrachtung vorhandener Forschungsarbeiten erscheint insbesondere das Fehlen von Forschungsarbeiten explizit zur Anwendung von Subkulturtheorien auf Hacker als bemerkenswert, wird das Etikett „(kriminelle) Subkultur“ doch regelmäßig dieser Zielgruppe zugeschrieben (u. a. Holt, 2014; Steinmetz, 2015; Wible, 2003; Yar, 2005a). Auf einen diesbezüglichen Forschungsbedarf hat Kempa (2006) hingewiesen.

In der deutschsprachigen Kriminologie ist Cybercrime insbesondere in der Form der Cybercrime im engeren Sinne auch im Jahr 2015 noch kaum präsent, auch wenn sich in den Lehrbüchern der klassischen Kriminologie wie bei Kaiser (1996[!]) oder Neubacher (2011) vereinzelte Hinweise bzw. kurze Kapitel finden. Die Ausführungen bei Neubacher (2011) liefern über die Skizzierung von Phänomenen hinaus mit dem Routine-Aktivitäts-Ansatz auch Hinweise für ein – allerdings aus Opferperspektive gestaltetes – präventives Handeln. Darüber hinaus sei auf eine Arbeit von Meier (2012) hingewiesen, die sich umfassend mit den Herausforderungen für Kriminologie und Kriminalität zur Schaffung von Sicherheit im Internet befasst.

Nach Meier (2012: 197) gibt es auf der Basis der wenigen vorliegenden Befunde

> „… keinen Anlass … davon auszugehen, dass die Internetkriminalität … anderen Regelmäßigkeiten folgt als sie aus der allgemeinen Kriminologie

> bekannt sind. Dazu gehören namentlich das häufigere Auftreten leichter als schwerer Delikte, die höhere Belastung junger Menschen, namentlich von Jugendlichen (digital natives), die höhere Belastung von Männern gegenüber Frauen sowie ein vergleichsweise geringer Anteil von Mehrfach- und Intensivtätern gegenüber einer Dominanz von Einmal- und Gelegenheitstätern. Flächendeckende Untersuchungen liegen zu diesen Fragen allerdings (noch) nicht vor …".

Die erstgenannten Erkenntnisse werden tendenziell durch die vorliegende Literaturanalyse bestätigt. Sie sind insofern interessant, als dass sie geradezu einladen, klassische Erklärungsansätze der Kriminologie auf ihre Anwendbarkeit bei der Cyberkriminalität zu prüfen und in diesem Kontext insbesondere auf die Jugenddelinquenz bzw. deren kriminologische Erklärungen zu fokussieren (so auch Yar, 2005a). Gerade dieser Diskurs würde allerdings den Rahmen dieser Arbeit sprengen, zumal Cybercrime im engeren Sinne bislang kaum im Kontext allgemeiner Jugenddelinquenz diskutiert wird und entsprechende Arbeiten in der Literatur weitestgehend zu fehlen scheinen.

Darüber hinaus ist prüfenswert, in welchen Bereichen ggf. neue oder hybride Erklärungen notwendig sein könnten (Nhan und Bachmann, 2015). Einen solchen neuen Erklärungsansatz hat Jaishankar mit der „Space Transition Theory" deshalb entwickelt, weil traditionelle Theorien aus seiner Sicht die Cyberkriminalität nur unzureichend erklären können (Jaishankar, 2008).

6.1 Bindungstheorie und Theorie der Selbstkontrolle

Kontrolltheorien liefern Erklärungen für das Phänomen, dass Menschen trotz weitverbreiteter Motivation häufig selbst gute Gelegenheiten zur Begehung strafbarer Handlungen nicht nutzen (Hess und Scherer, 2003). Einen Hinweis auf eine mögliche Anwendbarkeit der sozialen Kontroll- und Bindungstheorie von Travis Hirschi (1969) liefert Bachmann (2010) mit einer Befragung von Hackern (n=124) anlässlich der Hackerkonferenz ShmooCon 2008 in Washington D.C. Gemäß diesem theoretischen Ansatz ist der Grad der Einbindung eines Individuums in die Gesellschaft der Maßstab für die Angepasstheit seines Verhaltens. Bindung vollzieht sich dabei auf vier unterschiedlichen Ebenen: dem emotionalen Band zu bedeutenden Bezugspersonen („attachment"), einer konventionellen Zielen verpflichteten Lebensplanung („commitment"), beruflicher Einbindung und klar strukturierter Freizeit („involvement") sowie der inneren Billigung des konventionellen Wertesystems („belief") (Bock, 2015).

In der Befragung haben beschäftigungslose Hacker eine signifikant höhere Anzahl an Hackingversuchen als die beruflich eingebundenen Hacker berichtet. Grund dafür dürfte sein, dass Hacking eine sehr zeitintensive Beschäftigung ist und diese Zeit gerade arbeitslosen Hackern eher zur Verfügung steht. Zudem schaffen stabile Arbeits- und Karrierebeziehungen starke Verbindungen in die Gesellschaft Die Mehrzahl der Studenten im Sample waren Teilzeitstudenten mit Vollzeitjobs (Bachmann, 2010).

Ohne auf die Kritik an der Bindungstheorie insgesamt im Detail einzugehen (vgl. dazu Diedrich, 2013), sei hier lediglich der Aspekt aufgegriffen, dass die Theorie jegliches

abweichendes Verhalten mit fehlenden Bindungen an bestimmte Konventionen erklärt (ebd.). Deliktsspezifische Differenzierungen oder ein isolierter Fokus auf Hacker sind innerhalb dieses theoretischen Rahmens nicht möglich. Damit sind auch keine spezifischen Interventionen für Hacker ableitbar.

Die von Gottfredson und Hirschi (1990) auf der Basis der Bindungstheorie nachfolgend entwickelte allgemeine Theorie der Selbstkontrolle bzw. allgemeine Verbrechenstheorie („A General Theory of Crime“) sagt im Kern aus, dass Kriminalität eine Folge zu geringer Selbstkontrolle ist, weil Personen die unmittelbare Befriedigung von Bedürfnissen in den Vordergrund stellen, ohne die längerfristigen negativen Konsequenzen dagegen abzuwägen. Dieser umfassende theoretische Ansatz ist zwar auf Hacker anwendbar (UNODC, 2013), allerdings nicht isoliert auf Hacker, sprechen sich Gottfredson und Hirschi doch explizit gegen die These einer Spezialisierung unter Tätern aus und distanzieren sich ebenso von einer Differenzierung verschiedener Arten abweichenden Verhaltens (Diedrich, 2013). Damit könnte man im Umkehrschluss allerdings auch fragen, ob Hacker nicht durch weitere Formen abweichenden Verhaltens auffallen müssten. In diesem Kontext sei auf eine laufende niederländische Untersuchung verwiesen (Kranenbarg, 2014), in der u. a. durch Längsschnittvergleiche untersucht wird, ob Cyberkriminelle eine eigenständige Tätergruppe darstellen, die sich von Tätern in eher traditionellen Kriminalitätsbereichen unterscheiden.

Abschließend sei erwähnt, dass die Anwendbarkeit von Kontrolltheorien (im Zusammenspiel mit Lerntheorien) auch im Umkehrschluss möglich ist. Wem (als Hacker) aus seinem sozialen Umfeld und ggf. auch von staatlicher Seite signalisiert wird, dass auf Straftaten vielleicht nicht positiv aber doch nur wenig punitiv reagiert wird, ist erfahrungsgemäß nur allzu leicht bereit, seine Hemmungen zu überwinden und den Schritt von der Motivation zur Tat zu machen (Hess und Scherer, 2003). In diesem Kontext haben Ergebnisse aus Hackerbefragungen Relevanz, nach denen das Risiko einer Bestrafung als eher gering eingestuft wird (Chiesa et al., 2009; Young et al., 2007) und ehemalige Hacker gutbezahlte Tätigkeiten in der IT-Industrie finden (Sharma, 2007)(vgl. auch Kapitel 4.2.13).

6.2 Lerntheorien

Die Relevanz lerntheoretischer Ansätze im Zusammenhang mit Hacking ist bereits angedeutet worden. Lerntheorien gehen vereinfacht davon aus, dass sowohl legales als auch illegales Verhalten erlernt wird (Aebersold, 2007; Lösel und Schmucker, 2008). Der nachfolgende Abschnitt gibt keinen vollständigen Überblick über lerntheoretische Ansätze, sondern konzentriert sich auf eine Auswahl der sozialen Lerntheorien, die im Zusammenhang mit dem Hacken in der Literatur genannt sind. Herangezogen werden hier in erster Linie die Theorie der differentiellen Assoziation (auch Theorie der differentiellen Kontakte genannt) von Sutherland (1947) sowie die darauf aufbauende Theorie der differentiellen Verstärkung von Burgess und Akers (1966). Die Relevanz weiterer Lerntheorien wie die Theorie der operanten Konditionierung von Skinner (1953) oder die sozial-kognitive Lerntheorie von Bandura (1979) soll dies nicht schmälern.

Nach der von Edwin Sutherland (1947) entwickelten Theorie der differentiellen Assoziation existieren in einer modernen Gesellschaft unterschiedliche Strukturen von Normen und Verhaltensweisen. Ein junger Mensch kann demnach in Abhängig davon, mit welchen engen Gruppenkontakten er bzw. sie aufwächst, eher gesetzestreues oder aber abweichendes

Verhalten erlernen. Dies geschieht durch Interaktion in intimen Gruppen. Neben den Motivationen zur Begehung einer Straftat werden auch Techniken der Begehung erlernt. Von Bedeutung sind in diesem Lernprozess Aspekte wie Häufigkeit, Dauer, Priorität und Intensität der Kontakte und die Interaktionen zu sozial abweichenden Personen. Im Ergebnis werden Menschen dann kriminell, wenn bei ihnen Einstellungen, die Gesetzesverletzungen begünstigen, gegenüber Einstellungen, die Gesetzesverletzungen im Wege stehen, überwiegen (Eifler et al., 2001).

Burgess und Akers (1966) haben die Theorie der differentiellen Assoziation zu einer Theorie der differentiellen Verstärkung erweitert, indem sie spezielle Lernprozesse aufgezeigt haben, mittels derer sich die Wirkung der differentiellen Assoziationen erklären lässt (Eifler et al., 2001). Sie haben dabei auch auf die Theorie der operanten Konditionierung von Skinner (1953) zurückgegriffen, nach der – verkürzt formuliert – Handeln Ergebnis einer wiederholt positiven Bestärkung oder einer Ablehnung oder Bestrafung ist.

Burgess und Akers (1966) argumentieren, dass Kriminalität in einem Prozess erlernt wird, der aus den vier Stufen (1) „Differentielle Assoziation“, (2) „Differentielle Verstärkung“, (3) „Definitionen“ und (4) „Imitation“ besteht. Eingebunden in Lernumgebungen orientieren sich Personen zunächst daran, inwieweit in ihrer Gruppe eher konforme oder deviante Verhaltensweisen überwiegen, an denen sie sich orientieren können (Differentielle Assoziation). Unter „differentielle Verstärkung“ wird die Bestrafung respektive Belohnung verstanden, die als Ergebnis der Beteiligung an dem jeweiligen Verhalten erfahren wird. Daran gekoppelt sind positive bzw. neutralisierende wie negative Einstellungen bzw. Bewertungen (Definitionen). Abschließender Bestandteil ist die daraus erfolgende Nachstellung oder Imitation eines Verhaltens (Eifler, 2009).

Bezogen auf P2P-Musikdownloads hat Fisk (2006) gezeigt, dass alle vier der bei Burgess und Akers (1966) genannten Lernelemente einen signifikanten Einfluss auf das Verhalten haben. Im Prinzip kann damit gesagt werden, dass die Wahrscheinlichkeit illegaler P2P-Downloads steigt, je öfters junge Menschen derartiges Verhalten beobachten, je weniger sie dieses als falsch ansehen und je weniger sie befürchten, gefasst zu werden. Betrachtet man Hackercommunities bzw. Hackersubkulturen mit ihrer Hackerethik, mit ihren Möglichkeiten von Nachahmung und Modellierung aber auch die in dieser Arbeit genannten motivatorischen Aspekte, so wird deutlich, dass sich die Theorie der differentiellen Verstärkung auch zur Erklärung des Hackens an sich eignen sollte.

6.3 Neutralisationstheorie

In einem engen Zusammenhang mit Ansätzen des Subkultur wie auch des sozialen Lernens steht die von Gresham Sykes und David Matza (1957) entwickelte Neutralisationstheorie. Junge Menschen, die abweichendes Verhalten zeigen, haben regelmäßig keine geschlossene sub- oder gegenkulturelle Wert- und Vorstellungswelt, sondern in sich widersprüchliche und ambivalente Vorstellungen. Zeigen sie abweichendes Verhalten, so helfen ihnen bestimmte Rechtfertigungstechniken, ihr Handeln in Einklang mit dem herrschenden Normen- und Wertesystem zu bringen und ihre Schuld zu neutralisieren (Bock, 2015).

Sykes und Matza haben ursprünglich fünf Techniken der Neutralisation benannt: (1) Ablehnung der Verantwortung, (2) Verneinung des Unrechts, (3) Ablehnung des Opfers, (4) Verdammung der Verdammenden, (5) Berufung auf höhere Instanzen (vgl. Bock, 2015). Die Theorie wurde im Laufe der Zeit auf der Basis von Forschungserkenntnissen um weitere Neutralisierungsansätze ergänzt. Dazu gehören (6) die eher kaufmännische Begründung, dass die kriminelle Tat zu rechtfertigen sei, da man ja bereits eine große Zahl guter Taten vollbracht habe, (7) die Ablehnung der Notwendigkeit eines Gesetzes, (8) die Behauptung, dass alle anderen es auch tun und (9) die Befugnis bzw. den Anspruch zu besitzen, etwas zu tun (Moore, 2011). In methodischer Hinsicht sei auf die Schwierigkeit hingewiesen, in temporaler Hinsicht *ex ante*-Motivationen von *ex-post*-Rechtfertigungen zu unterscheiden (Moore, 2011; Yar, 2005a).

Bereits das 1986 verfasste „The Hacker's Manifesto" enthält mit seinen ethisch-moralischen Grundaussagen auch eine Reihe von Rechtfertigungen bzw. Neutralisationsmöglichkeiten für Hacker (Yar, 2005a). Dort finden sich die Argumente, dass intelligente Schüler unter Langeweile leiden, weil sie durch inkompetente und sadistische Lehrer unterrichtet werden oder aber als verdammte Kinder, die doch alle gleich sind, dauerhaft abgelehnt werden. Weitere Argumente beziehen sich auf die Möglichkeit, Dienste zu nutzen, die billig sein könnten, wenn sie nicht von „geschäftemacherischen Vielfraßen" betrieben würden oder auf den Hinweis, nicht lernen und forschen zu dürfen, weil sie, die Urheber von Atombomben, Kriegen, Mord und Betrug, dies ablehnten.

Rogers (2001) wies darauf hin, dass Selbstzensur beim Hacking dadurch ausgeschaltet werden kann, dass man Opfern das Menschliche nimmt bzw. die Schuld den Opfern zuschiebt. Rogers (wie in Fötinger und Ziegler, 2004, zitiert) geht zudem davon aus, dass Hacker dazu tendieren, die Konsequenzen ihres Handelns zu minimieren oder fehlzudeuten, indem sie darauf hinweisen, dass ihr Handeln einen Wert für die Organisation oder Gesellschaft an sich habe. Post (wie in Fötinger und Ziegler, 2004, zitiert) schreibt Hackern eine „ethische Flexibilität" zu, mittels derer die negativen Konsequenzen des eigenen Handelns ignoriert werden. Beispiel für diese argumentative Flexibilität von Hackern sind demnach Attacken gegen Pädophile (vgl. Chiesa et al., 2009 mit dem Beispiel der „Ethical Hackers Against Paedophilia"), wird hier doch das eigene strafbare Handeln in Bezug gesetzt zur gesellschaftlichen Ächtung des Opferhandelns (Kirwan und Power, 2013).

Weitere in der Literatur genannte Beispiele für ethische Rechtfertigungen sind Hacking zur Verbesserung der IT-Sicherheit durch Finden von Schwachstellen, Wissensgewinnung bei Schülern/Studenten und Schutz der Gesellschaft gegen große Firmen durch Sicherstellung eines freien Zugangs zu Informationen (Sharma, 2007). Besondere Relevanz dürften Neutralisierungstechniken ferner für Innentäter haben (Ann, 2012).

Die Neutralisierungstheorie wird insbesondere auch im Kontext von Pirateriedelikten genannt, insbesondere dem Filesharing beispielsweise von Musik oder Filmen. In einer Studie von Moore (2011) nutzten die Studienteilnehmer sechs der o. g. Neutralisierungstechniken zur Rechtfertigung ihres Handelns, wobei teilweise auch mehrere Techniken gleichzeitig genannt worden waren. Die am häufigsten benutzten waren Verneinung des Unrechts, Ablehnung des Opfers und der Hinweis, dass alle anderen es auch tun.

Über den Ansatz der situativen Kriminalprävention besteht die Möglichkeit, Neutralisierungsmöglichkeiten zu nehmen, in dem mittels des Prinzips „Entschuldigungen beseitigen" potenziellen Tätern im Kontext einer spezifischen Tatgelegenheit vermittelt wird,

dass weiteres Verhalten strafbar ist (vgl. dazu Kapitel 7.6).

6.4 Theorie des rationalen Wahlhandelns

Ökonomische Kriminalitätstheorien gehen grundsätzlich davon aus, dass Kriminalität nichts Krankhaftes oder Unnatürliches, sondern das Ergebnis einer „menschlichen Handlungswahl" (Bock, 2015: 71) ist. In Anlehnung an Cesare Beccaria und Jeremy Bentham wird argumentiert, dass der Mensch jegliches und damit auch abweichendes Handeln in einem utilitaristischen, d. h. nützlichkeitsorientierten Ansatz nach Anreiz und Risiken bzw. Aufwand und Kosten bewertet. Dabei werden weder der Nutzen noch die Kosten einer Straftat allein in einem monetären Sinne bemessen; auch immaterielle Aspekte wie der Gefühlszustand nach einer Tat, beispielsweise das Hochgefühl nach einem Hack oder die durch die Tat erwarteten Nachteile lassen sich aus Tätersicht zweckrational bewerten (Akers, 1990; Hess und Scherer, 2003; Neubacher, 2011).

Die „rational choice"-Theorie ist insofern von großer Bedeutung auch für die Prävention, als dass beispielsweise Abschreckungseffekte in Form von Strafandrohungen in die Kosten-Nutzen-Kalkulationen (potenzieller) Täter einfließen sollen. Mittlerweile ist jedoch anerkannt, dass die Höhe der zu erwartenden Strafe aus Tätersicht weniger relevant ist als die subjektive Einschätzung des Entdeckungs- und damit auch des Sanktionsrisikos (Akers, 1990; Killias et al., 2009; Neubacher, 2011). Darüber hinaus ist anerkannt, dass Menschen nur begrenzt rationale Entscheidungen treffen, weil ihr Wissen z. B. über einen potenziellen Tatort oder das Setting einer geplanten Tat unvollständig ist und zudem Erregungen (durch Nervosität, Wut, Rachsucht etc.) das Treffen rationaler Entscheidungen verhindern (Akers, 1990; Cornish und Clarke, 1986).

Bezogen auf Hacker hat die Theorie insofern Relevanz, als dass diese Tätergruppe per se als „kopfgesteuert" angesehen wird. Die Ausführungen zur Motivation (Kapitel 4.2.9) haben allerdings gezeigt, dass auch für Hacker weitere, emotionale Aspekte durchaus eine bedeutende Rolle spielen können, so dass nicht immer mit in hohem Maße rationalen Tatausführungen zu rechnen ist, was durchaus Raum für polizeiliche Ermittlungen lässt. Befragungen und Aussagen von Hackern (vgl. Chiesa et al., 2009; Krebs, 2003) deuten an, dass diese nicht nur die Strafverfolgungsseite als nicht besonders kompetent empfinden, sondern sich im Vorfeld einer Tat generell kaum Gedanken hinsichtlich möglicher Strafaspekte machen (vgl. Kapitel 4.2.13). Eine in höherem Maße kompetente Strafverfolgung, die dazu führen würde, dass Täter eine erhöhte Wahrscheinlichkeit eines Strafverfahrens einkalkulieren müssten, sollte aus theoretischer Sicht auch eine präventive (Abschreckungs-) Wirkung entfalten können (Bachmann, 2010).

6.5 Routine-Aktivitätstheorie

Lawrence Cohen und Marcus Felson haben die Routine-Aktivitätstheorie („Routine activity theory" - RAT) 1979 aus der Erkenntnis abgeleitet, dass in den 60er Jahren Wohnungseinbrüche in den USA angestiegen waren, obwohl es den Menschen immer besser ging. Die zunehmende Kriminalität konnte eigentlich nur über veränderte Lebensgewohnheiten, Lebensstile und damit auch „Routineaktivitäten" erklärt werden. Dazu

gehörten neben einer zunehmenden Zahl an Singles auch zunehmend berufstätige verheiratete Frauen, die ihre Wohnungen oder Häuser tagsüber zum Arbeiten verließen und so in dem Umfang bislang nicht gekannte Tatgelegenheiten für Einbrecher schufen (Neubacher, 2011).

RAT-Theoretiker nehmen einen Hang zu abweichendem Verhalten als gegeben hin („take criminal inclination as given", vgl. Cohen/Felson, 1979: 589); aus ihrer Sicht gibt es keinen Mangel an Motivationen, egal aus welchem Grund, für delinquentes Verhalten. Sie lehnen soziale, ökonomische oder auch andere strukturelle Ursachenbündel gar nicht ab, sondern argumentieren lediglich, dass diese *alleine* nicht ausreichen, die Begehung einer einzelnen spezifischen Tat zu erklären.

Die RAT setzt als Voraussetzung einer Tat die räumliche und zeitliche Konvergenz dreier Bedingungen voraus: (1) ein motivierter Täter muss auf (2) ein geeignetes Ziel stoßen, (3) ohne dass geeignete Wächter oder Beschützer die Tat verhindern können (Cohen und Felson, 1979). Die RAT setzt zusätzlich voraus, dass Täter in ihrem Handeln nicht fremdbestimmt sind, sondern auf der Basis einer vorausschauenden Kalkulation der Kosten und Nutzen ihres Handelns agieren; es bestehen insofern deutliche Bezüge zur Theorie der Rationalen Wahl (Eifler et al., 2001; Neubacher, 2011; Yar, 2005b).

An dieser Stelle wird gerne eingeworfen (vgl. dazu Yar, 2005b), dass die RAT nicht in der Lage sei, Straftaten mit nicht-instrumentellen bzw. affektiven Motiven zu erklären. Ähnliche Probleme sehen Verfechter der „kulturellen Kriminologie", nach denen emotionale und affektive „Verführungen" zur Kriminalität, die junge Menschen in bestimmten Bereichen erfahren, nicht erklärt werden können (vgl. Katz, 1988). Eine Lösung dieses Problems könnte allerdings schon sein, von simplen ökonomischen Kosten-Nutzen-Argumentationen wegzukommen und mit einem umfassenderen Bild von Rationalität zu arbeiten. Dies würde es erleichtern, Handlungen auf der Grundlage von Furcht, Wut oder Aufregung, die ja nicht per se irrational sind, ebenfalls erklären zu können.

In den letzten Jahren ist die RAT vermehrt zur Erklärung unterschiedlicher Formen von Cybercrime herangezogen worden (so u. a. Chon und Broadhurst, 2014; Meier, 2012; Neubacher, 2011; UNODC, 2013; Yar, 2005b), auch wenn die Anwendbarkeit zum Teil in Frage gestellt wird (u. a. Bossler und Holt, 2009; Yar, 2005b). Eine regelmäßige Kritik greift die zeitlich-räumliche Dimension der RAT auf und argumentiert u. a., dass Endpunkte im Internet keine Distanz zueinander aufweisen, die virtuelle Welt quasi „anti-räumlich" und alles „nur einen Klick" voneinander entfernt sei (Yar, 2005b). Insofern gäbe es auch keine geografischen Grenzen wie in der realen Welt. Gegen eine derartige Sicht sprechen im Internet gängige Begrifflichkeiten wie „Portal", „Site", „back door", „Chat room", „lobby", „cafes", „superhighway" oder „mail" die einen deutlichen Raumbezug („spatiality") auch in der virtuellen Welt signalisieren. Yar (2005b) kommt zu dem Ergebnis, dass spatiale Gesetzmäßigkeiten auch in der virtuellen Welt gelten, die Veränderungsgeschwindigkeit dort allerdings verglichen zur realen Welt größer sei. Auch der Zeitfaktor spielt in der Cyberwelt vermutlich eine geringere Rolle als in der realen Welt, denn das Internet ist „24/7" bevölkert und für die Ausübung bestimmter Aktivitäten spielen Zeit bzw. zeitliche Rhythmen, die Täter antizipieren müssten, kaum eine Rolle (ebd.).

Im Ergebnis ist von einer immer größer werdenden Zahl an angreifbaren „geeigneten Zielen" auszugehen, die mit der zunehmend online verbrachten Zeit und der zunehmenden Nutzung von in das Internet verlagerten Dienstleistungen wie Bankanwendungen, Einkaufmöglichkeiten oder Portalen für das Streamen von Musik und Filmen entstehen.

Soziale Netzwerke wie Twitter oder Facebook offenbaren potentiellen Tätern ebenfalls hunderte von Millionen von möglichen Opfern für jedwede Art von Betrügereien, Erpressungen etc. Gerade soziale Netzwerke offerieren potenziellen Täter darüber hinaus ausreichend Informationen über mögliche Opfer, um diese möglichst zielgerichtet angehen zu können (UNODC, 2013).

Bezogen auf die Bedingung „motivierter Täter“ haben Chon und Broadhurst (2014) Ressourcenaspekte untersucht und sind zu dem Ergebnis gekommen, dass eine Prävalenz bestimmter Formen von Cyberkriminalität allein schon aufgrund der Verfügbarkeit einfach zu nutzender, praktisch fertig verpackter Softwarelösungen anzunehmen ist, die für kriminelle Zwecke entwickelt und angeboten werden. Beispielhaft dafür können Programme genannt werden, die den Infektionsprozess von Computern automatisiert durchführen, sobald eine kompromittierte Webseite aufgesucht wird (Exploit-Bausätze), die die Kontrolle von „Zombie-Netzwerken“ (Botnet-Bausätze) ermöglichen, die die Detektion von Malware verhindern sollen (Crypter) oder die als Keylogger heimlich persönliche Daten beim Eingeben in die Tastatur abgreifen (Chon und Broadhurst, 2014). Die Autoren haben in ihrer Arbeit unterschiedliche Erklärungsmodelle für ihr Konzept des ausreichend ausgestatteten Täters entworfen, die Täterressourcen als bei Tatbegehung externe Größe (z. B. Einsatz von Exploit-Kits) oder auch als vom Täter selbst erworbenes Wissen (einschließlich Fähigkeiten zur Rechtfertigung des eigenen Handelns) interpretieren, ohne dass die Validität der Modelle bereits überprüft und Ableitungen für die Praxis erarbeitet wurden.

Bezogen auf die Bedingung „geeigneter Wächter bzw. Beschützer“ als drittes Wesensmerkmal der RAT sei angemerkt, dass eine Wächterschaft nicht nur durch Aktivitäten, sondern bereits durch alleinige physische Präsenz bewirkt werden kann. Handelt es sich bei dem Wächter um eine Person, dann erinnert dieser potenzielle Täter daran, dass jemand die Tat wahrnehmen könnte. Wächter können sowohl formeller als auch informeller Art sein, wobei die RAT insbesondere die Bedeutung informeller Agenten betont. Über diese soziale Wächterschaft hinaus werden physische Sicherheitsmechanismen wie Sicherungen, Türen, Alarme usw. als bedeutsam angesehen. Insgesamt ist die Abwesenheit oder Präsenz eines Wächters zu der Zeit und an dem Ort, an dem potenzielle Täter und Opfer zusammenkommen, als der kritische Aspekt anzusehen, der über die Tatbegehung entscheidet (Yar, 2005b).

Die Cyberwelt kennt wie die reale Welt eine Reihe von privaten bzw. informellen Wächtern. Dazu zählen bspw. Netzwerkadministratoren, Sicherheitspersonal im IT-Bereich, Handelsorganisationen mit Selbstverpflichtungen bis hin zu Privatpersonen, die auf sozialen Netzwerken oder online-Plattformen andere Teilnehmer bewerten. Zusätzlich zu diesen sozialen Wächtern existiert ein breites Spektrum an physikalischen bzw. technologischen Wächtern, automatische Agenten, die Systeme permanent überwachen wie bspw. Firewalls, Intrusion Detection-Systeme, Virusscanner etc. (Yar, 2005b). Einen umfassenden Überblick über den Forschungsstand zum Thema bieten Hartel et al. (2011).

Die RAT ist Präventionsaspekten eine überaus wichtige Theorie, bietet sie doch direkte Hebel für eine situative Prävention nicht nur in technischer Hinsicht (Cornish und Clarke, 2003; Hartel et al., 2011; Hartel, 2014; Neubacher, 2011; Willison, 2005).

6.6 Kriminalität als „verbotene Frucht“

Im Ergebnis kann zwar eine Tat am Ende immer als Ergebnis eines Entscheidungsprozesses der rationalen Wahl erklärt werden. Es stellt sich dennoch die Frage, ob eine derartige Interpretation in jedem Fall sinnstiftend ist, wenn es über den instrumentellen Aspekt hinaus um Fragen der Emotionen oder auch der Expressivität (bei) der Tatausführung geht.

Katz (1988) hat in seinem Werk „Seductions of Crime“ bisherige Ansätze aus Lern- und psychologischen Theorien dahingehend weitergedacht, Kriminalität als „verbotene Frucht“ zu porträtieren. Bisherige kriminologische Ansätze, die sich mit den sozialen Ursachen von Kriminalität befassen, stellt er genauso wie den rationalen Akteur in Frage und konzentriert sich stattdessen auf die „Magie der Motivation“ (Hess und Scherer, 2003) und damit auf Emotionen und Bedeutungen, die Kriminalität für den Einzelnen hat. Viele Delikte gerade der Jugenddelinquenz sind rational wie materiell nicht erklärbar, sondern allenfalls durch die zusätzliche Aufregung oder Lust, die sie bieten. Kriminalität ist insoweit auch die Suche nach hedonistisch geprägter Identität (Veil, 2008). Strafen wirken in diesem Kontext nicht abschreckend, sondern in Teilen als Herausforderung.

Aus der Phänomenologie des Hackings mit einem hohen Anteil an jugendlichen Hackern und einem Motivbündel, in dem Aspekte wie Spaß am Hacken, Unterhaltung („entertainment“) und auch Nervenkitzel („thrill“) nicht fehlen, lässt sich die Anwendbarkeit von Katz‘ Erklärungsansatz ableiten (so auch Grabosky, 2000). Die Literatur bietet darüber hinaus allerdings nur wenig Hinweise, welche Schlussfolgerungen daraus für Maßnahmen der Intervention und Prävention ableitbar sind.

6.7 Flow-Theorie

Im Zusammenhang mit intrinsischen Anreizstrukturen bzw. Motivationen bezeichnet Flow das Gefühl der völligen Vertiefung und des Aufgehens in einer Tätigkeit, in der Hunger, Müdigkeit und alles über die ausgeführte Tätigkeit hinaus vergessen wird. Csikszentmihalyi hat das Konzept des Flow in den 1970er Jahren im Hinblick auf Risikosportarten entwickelt. Bereits vorher war das Phänomen aus der Spielwissenschaft bekannt. Heute findet das Konzept über körperliche Tätigkeiten hinaus auch im Bereich rein geistiger Aktivitäten Anwendung (Wikipedia). Definierendes Merkmal von Flow ist die intensive Befassung mit einer Tätigkeit, bei der die volle Aufmerksamkeit dieser Tätigkeit gewidmet und die handelnde Person in höchstem Maße beansprucht ist – ohne sich bereits überfordert zu fühlen (Csikszentmihalyi, 2007; Csikszentmihalyi et al., 2005).

Bezogen auf Hacker finden sich im Jargon File (Vers. 2.1.1. v. 12.06.1990) Hinweise auf das Erreichen eines Flowzustandes, der mit dem Begriff „hack mode“ bzw. „deep hack mode“ als „*… a Zen-like state of total focus on the problem which may be achieved when one is hacking...*“ beschrieben wird.

In einer Befragung von (n=457) russischsprachigen Hackern zur Nutzung von Informationstechnik und spezifischen Flow-Erfahrungen (Voiskounsky und Smyslova, 2003) zeigte sich ein Flow-Erleben nur bei den kompetentesten sowie den am wenigsten kompetenten Hackern; im Mittelfeld der Möchtegern- und Gelegenheitshacker gab es nur wenig Flow-Erfahrungen. Während bei den Möchtegernhackern zu hohe Herausforderungen auf zu niedrige Fertigkeiten trafen, war es bei den Gelegenheitshackern umgekehrt; hier gab

es kaum passende Herausforderungen für ein hohes Fertigkeitsniveau. Steinmetz (2015) bestätigt die Ergebnisse auf der Basis einer ethnografischen Untersuchung insofern, als dass Hacker um überhaupt in einen Flow Zustand zu kommen, Fertigkeiten benötigen, die sich erst nach längerer Zeit des Hackings entwickeln. Auf der Basis beider Untersuchungen (Voiskounsky und Smyslova, 2003; Steinmetz, 2015) kann festgehalten werden, dass Flow nicht linear mit der Zunahme an Fertigkeiten ansteigt, sondern sich Phasen des Flow abwechseln mit Phasen der Krise und erneuten Phasen des Flow. Flow-Erfahrungen führen auch dazu, dass Hacker nach noch größeren Herausforderungen suchen (Chiesa et al., 2009). Insoweit sind sie Extremsportlern vergleichbar.

Woo (2003) geht davon aus, dass Hacker mit einem hohen Flow-Niveau mit höherer Wahrscheinlichkeit in die Computer anderer Menschen einbrechen und Webseiten verändern als Hacker mit einem niedrigen Flow-Niveau. Rheinberg und Tramp (2006) haben in dem Kontext eine Korrelation sowohl zwischen der leistungsthematischen Anreizskala (Kompetenzerleben bzw. Kompetenzerweiterung) wie auch der rebellisch-destruktiven Anreizskala (Rebellische Illegalitätstendenz/Sensation Seeking/Prestigesuche) und dem Erfahren von Flow (mit jeweils r=.38) nachgewiesen. Wem also die unerkannten Möglichkeiten des Computers zur Herbeiführung von Schäden sowie Sensation Seeking wichtig sind, der berichtet über Flow. Die „vernünftige Vielseitigkeit“ der Computernutzung wie auch die Wertschätzung gemeinschaftlicher Computererlebnisse können laut Rheinberg und Tramp (2006) keine Flow-Erfahrungen vermitteln. Unter Präventionsaspekten bedeutsam ist die Erkenntnis, dass Flow sowohl bei hacker- als auch bei crackertypischen Computernutzungen erlebt wird. Flow ist nicht auf destruktive Tätigkeiten am Computer beschränkt, sondern lässt sich auch durch eine an legalen Zielen orientierte leistungsmotivierte Hackeraktivität erreichen (ebd.).

Rennie und Shore (2007) zeigen am Beispiel der geringen Anklagezahlen von Cybercrime in den USA für den Zeitraum August 2003 bis August 2004 allerdings, dass kaum Taten aus dem Antrieb purer Freude („fun“) heraus ausgeführt wurden. Die Mehrzahl der Fälle ließ sich aus ihrer Sicht mit dem Flowmodell alleine nicht erklären. So unterscheiden sich doch beispielsweise Cyberterroristen, Hacktivisten, Penetrationstester und Cyberkrieger aus motivationaler Sicht zum Teil fundamental voneinander.

6.8 Space Transition Theory

Annahme der von Jaishankar (2008) entwickelten Space Transition Theory (STT) ist, dass sich Menschen in der Cyberwelt anders als in der realen Welt verhalten. Die Theorie versucht diese Unterschiede bzw. das Verhalten von Menschen zwischen den beiden Welten zu erklären.

Postulate der Space Transition Theory sind folgende (vgl. Jaishankar, 2008):

(1) Menschen, die delinquentes Verhalten in der realen Welt aufgrund von Status und Position unterdrücken, sind geneigt, derartiges Verhalten in der Cyberwelt zu zeigen.

(2) Flexible Identitäten, eine dissoziative Anonymität und unzureichende Abschreckungsfaktoren in der Cyberwelt eröffnen Chancen der Tatbegehung.

(3) Kriminelles Verhalten von Tätern im Cyberraum dürfte in die reale Welt importiert werden und umgekehrt.

(4) Wechselnde Unternehmungen von Tätern in den Cyberraum und die dynamisch räumlich-zeitliche Natur des Cyberraumes bieten Chancen der Flucht.

(5) a) Fremde dürften sich im Internet zusammentun, um in der realen Welt Taten zu begehen.

b) Mittäter in der realen Welt dürften sich zusammentun, um in der Cyberwelt Straftaten zu verüben.

(6) Personen aus geschlossenen Gesellschaften dürften mit größerer Wahrscheinlichkeit Straftaten im Cyberraum begehen als Menschen aus offenen Gesellschaften.

(7) Der Konflikt von Normen und Werten der realen Welt mit den Normen und Werten der Cyberwelt kann zu Cyberkriminalität führen.

Eine kritische Diskussion dieser Theorie findet sich in der Literatur bislang genauso wenig wie valide empirische Überprüfungen. Die Ergebnisse einer Arbeit von Danquah und Longe (2011) zeigen lediglich, dass Cybercrime in Ghana weitgehend von Betrug dominiert ist und die Postulate der Theorie nicht auf alle Formen von Cybercrime anwendbar sind.

Dass es sich durchaus lohnen würde, die Theorie zu überprüfen, zeigt die Untersuchung von Chiesa et al. (2009), nach denen Hacker im offline-Leben wohl eher schüchtern sind, während sie in ihrem „natürlichen Element“, der Cyberwelt, eine völlig andere Persönlichkeit offenbarten. Viele befragte Hacker kommunizieren sehr leicht auf elektronische Weise mit anderen, während diese Ungezwungenheit im richtigen Leben fehlt. Die Autoren erklären dies damit, dass das elektronische Medium als Barriere wirkt, die den Menschen versteckt und auch schützt. Die Autoren relativieren ihre Aussagen allerdings insoweit, als dass die festgestellten Verhaltensunterschiede im Netz und in der realen Welt nicht nur für Hacker, sondern auch für andere Heranwachsende gelten.

Meier (2012) hat darauf hingewiesen, dass es die im Netz geschaffene Distanz von Täter und Opfer ist, die Kriminalität begünstigt. Er vermutet hier, dass die fehlende Wahrnehmung eines oder einer Geschädigten täterseitig zur Absenkung von Hemmschwellen führt.

6.9 Zwischenfazit

Der Begriff der Cyberkriminalität umschreibt zwar ein an sich recht junges Kriminalitätsphänomen, wobei für Cybercrime im weiteren Sinne gilt, dass Computer oder Informationstechnik lediglich neue Tatmittel für an sich bekannte Delikte wie den Betrug, die Erpressung, Verstöße gegen das Urheberrecht oder auch die Kinderpornographie darstellen. Daraus ableitbar ist die Anwendung der zeitgenössischen Kriminalitätstheorien mit all ihren Stärken und Schwächen (vgl. dazu exemplarisch Kaiser, 1996).

Da auch das Hacken bzw. Cybercrime im engeren Sinne kein an sich neues menschliches Verhalten beschreibt, sondern dieselben menschlichen Antriebskräfte wirken, die Menschen auch in anderen Bereichen antreiben und dort auch zur Höchstleistung motivieren, ist die

Anwendbarkeit derselben kriminologischen Erklärungen ebenfalls kaum überraschend. Dem steht nicht entgegen, dass kriminologische Theorien nicht abschließend erklären können, warum sich Menschen in Richtung strafbaren Hackings bewegen. Sie vermögen lediglich Einzelfragen psychologischer, sozialer, kultureller oder auch situativer Art erklären. Den Mehrwert, den sie in dieser Hinsicht haben können, gilt es auszubauen, in dem aus Strafverfolgungssicht wie aus Präventionssicht relevante Fragestellungen formuliert werden, denen sich die kriminologische Forschung unter Fokussierung auf die phänomenspezifischen Aspekte von Cybercrime i.e.S. in enger Abstimmung mit der Strafverfolgungspraxis widmen kann.

7 Täterorientierte Handlungsmöglichkeiten

In dem nun folgenden letzten inhaltlichen Teil der Arbeit werden täterorientierte Handlungsmöglichkeiten aufzeigt. Die nachfolgenden Maßnahmen beschränken sich auf diejenigen Informationen, die in der öffentlich zugänglichen Literatur publiziert wurden (sog. Open Sources-Quellen). Ausgangspunkte sind weder polizeiinterne Quellen noch weitergehende Aktivitäten wie beispielsweise Verfahren des Brainstormings.

In inhaltlicher Hinsicht werden sowohl repressive als auch präventive Möglichkeiten genannt. Auf eher allgemeine Handlungsnotwendigkeiten beispielsweise der internationalen polizeilichen Zusammenarbeit oder der Fortentwicklung des Rechts, die sich im Kern auf die Tat als solche und nicht allein auf den Täter beziehen, wird hier allerdings nicht eingegangen.

7.1 Durchführung von sozialen Netzwerkanalysen

Die soziale Netzwerkanalyse (SNA) ist eine Methode der empirischen Sozialforschung, die der Erfassung, systematischen Analyse und quantifizierenden Beschreibung sozialer Beziehungen und sozialer Netzwerke dient. Maßzahlen (wie Zentralität und Dichte) helfen dabei, auch komplexe Netzwerke zu verstehen (Wikipedia). Möglichkeiten sind die Auswertung von Blogs sozialer Netzwerke oder (IRC-)Kommunikationen, über die sich eine Fülle personenbezogener Faktoren wie Alter, Geschlecht, Bildungsstand, Fertigkeiten, Wohnort, Gruppenzugehörigkeit, Kommunikation, Vertrauen etc. gewinnen lassen (Décary-Hétu und Dupont, 2012; Dupont, 2013; Holt et al., 2009 & 2012; Holt und Kilger, 2012).

So zeigten beispielsweise die Ergebnisse der Untersuchung der sozialen Netzwerke einer Gruppe russischer Hacker, dass selbst einige der „higher threat actors“ nicht nur den Ort, in dem sie aktuell lebten, anzeigten, sondern auch allgemeine persönliche Interessen im Internet offenbarten. Dies wird mit der Notwendigkeit erklärt, auch Kontakte zu anderen Personen, die außerhalb der Hacker-Subkultur operieren und im selben Ort leben, zu ermöglichen (Holt et al., 2009 & 2012).

Décary-Hétu und Dupont (2012) argumentieren, dass die SNA notwendige wissenschaftliche und objektive Messungen von Netzwerkstrukturen bereitstellt einschließlich der Informationen über die Stellung ihrer Schlüsselpersonen. Sie helfen u. a. dabei, die notwendigen Ressourcen besser abschätzen bzw. unter Ressourcenaspekten Handlungsalternativen besser bewerten zu können, die für die Zerschlagung von kriminellen

Netzwerken notwendig sind. Dabei sind allerdings grundsätzliche ethische und rechtliche Aspekte zu berücksichtigen.

7.2 Einsatz der Kriminalitätsskriptanalyse

Einige Autoren (Willison, 2005; Hutchings und Holt, 2015) schlagen die Analyse von Tatstrukturen auf der Basis von Kriminalitätsskripten („crime scripts“) vor, einer Methode, die von Cornish (1994) entwickelt wurde. Kriminalitätsskripte beschreiben in einer Sequenzanalyse die zur Vorbereitung, Durchführung und Beendigung einer Straftat erforderlichen Handlungen. Sie sind damit zugleich Abbild der täterseitigen Entscheidungsfindungsprozesse im Zusammenhang mit einer Tat in all ihren Phasen (ebd.).

Ziel der Skriptanalyse ist insoweit die Organisation von verhaltensspezifischen Informationen in einen chronologischen Ereignisablauf. Als einfaches Beispiel sei ein „Restaurant Skript“ genannt, das Gäste eines Restaurants befolgen: Restaurant betreten, Tisch aussuchen, bestellen, essen, Rechnung bezahlen und das Lokal wieder verlassen. Neben universellen Skripten, für die beispielhaft das „Restaurant Skript“ steht, sind auch spezifizierte Skripte („tracks“) möglich (z. B. „fast food *track*“, „cafeteria *track*“)(Cornish, 1994: 159). Das Skript hat eine feste Reihenfolge, so kann man nicht essen ohne vorher einen Tisch gefunden zu haben. Das Skript verfolgt eine rational zielorientierte Handlung, wird allerdings wie auch eine Rezeptur zum Kochen nicht immer strikt befolgt. Akteure sind in der Lage zu improvisieren, sofern ihre auf einen Erfolg der Handlung ausgerichtete Wahrnehmung dies notwendig macht (Hutchings und Holt, 2015; Willison, 2005).

Die Erstellung eines Skriptes setzt ein möglichst umfangreiches Wissen über den benutzten Modus Operandi wie auch über spezifische Täterentscheidungen voraus. Dazu zählen der Zugang zum Tatort, die für die Tat notwendigen Fertigkeiten, geleistete (finanzielle) Aufwände, Informationen über Tatgelegenheiten und benutzte Hilfsmittel (u. a. Werkzeuge, Waffen, Kommunikationsmittel) sowie die für die Tat notwendige technische Expertise. Die Erstellung eines Kriminalitätsskriptes basiert daher auf der Einbindung aller polizeilich relevanten Informationsquellen (Tompson und Chainey, 2011).

Die Skriptanalyse wurde bereits in unterschiedlichsten Kriminalitätsbereichen wie beispielsweise dem sexuell motivierten Kinderhandel, bei Raubstraftaten, dem Autodiebstahl und Graffiti, bei Sexualstraftaten und der Organisierten Kriminalität angewendet (Hutchings und Holt, 2015 – auch mit weiteren Literaturverweisen).

Hutchings und Holt (2015) haben die Kriminalitätsskriptanalyse zum besseren Verständnis von Online-Schwarzmärkten am Beispiel von drei englisch- und zehn russischsprachigen Foren angewandt. Dabei ging es, basierend auf dem universellen Skript von Cornish (1994), speziell darum, Täteraktionen identifizieren zu können, die notwendig sind, um auf derartigen Marktplätzen erfolgreich interagieren zu können. Analysiert wurden die Phasen der Vorbereitung (u. a. Aufsetzen von Software, Einrichtung von Accounts, Anonymisierung und Sicherheit), Zugang (Erlernen der Sprache und Regeln eines Marktplatzes), Vorbedingung (Beschaffung bzw. Erstellung eigener Produkte), instrumentelle Vorbedingung (Bewerbung von Produkten und Dienstleistungen, Unterwerfung von Verifikationsprozeduren für Produkte und Dienstleistungen), instrumentelle Eröffnung (Austausch von Informationen über Strafverfolgungsbehörden, Verhandeln und Kommunizieren), instrumentelle Verwirklichung (Versand und Empfang der Zahlung), Ausführung (Verpackung von Waren, Transport),

Nach-Bedingung (Reputationsmanagement, Austausch von Währungen), Beendigung (Geldwäsche).

Die Autoren (ebd.) sehen die Skriptanalyse als hilfreichen Weg hinsichtlich des Verständnisses des Funktionierens von Online-Schwarzmärkten an. Durch die damit dezidiert mögliche Beschreibung der Tatabläufe schafft ein derartiges Vorgehen Voraussetzungen für die Anwendung der situativen Kriminalprävention (vgl. Kapitel 7.6), mittels derer Prozesse aus Tätersicht verkompliziert bzw. Täter abgeschreckt werden.

7.3 Wirksamere Strafverfolgung

In Anwendung lerntheoretischer Ansätze in Kombination mit der Theorie der rationalen Wahl ist ein Augenmerk auf eine wirksamere Strafverfolgung zu legen, um nicht nur die Quote verurteilter Cyberstraftäter zu erhöhen, sondern um dadurch auch einen präventiven Abschreckungseffekt gegenüber dem illegalen Teil der Hackercommunity zu erzielen. Bachmann (2010) weist allerdings auch darauf hin, dass Abschreckung kein einfaches Unterfangen sei. So werden bei steigenden Cybercrime-Fallzahlen nur relativ wenige hochkarätige Fälle auch erfolgreich angeklagt, zumeist dann auch ohne schnelle und harte Bestrafung (Holt und Kilger, 2012). Diese Unsicherheit, dass es tatsächlich zu einer Bestrafung kommt, ist insoweit problematisch, als dass damit mögliche Abschreckungseffekte unterminiert werden. Wie diese Literaturanalyse (vgl. Kapitel 4.2.13) gezeigt hat, gehen viele Hacker tatsächlich nicht von einer Entdeckung und Bestrafung aus.

7.4 Störung illegaler Märkte

Verschiedene journalistische Arbeiten und Studien (u. a. Dupont, 2013; Infosec Institute, 2015; McCoy et al., 2012; Olson, 2012) deuten an, dass sich auch hochentwickelte Hackergruppierungen durch Muster von Misstrauen, Feindseligkeit und Vertrauensbrüche charakterisieren lassen. Auf den illegalen Schwarzmärkten des Internets hat dies dazu geführt, dass vergleichbar legalen Plattformen wie Amazon oder Ebay Reputationsmechanismen basierend auf Verkäufer- und Käufer-Bewertungen eingeführt wurden (Infosec Institute, 2015; Hutchings, 2014). In dem Kontext regt Holt (2013) weitere Forschungsarbeiten zu der Fragestellung an, inwieweit es möglich sei, über „Verleumdungsangriffe“ („slander attacks“) die Beziehungen und das Vertrauen zwischen Käufern und Verkäufern zu untergraben (aus: McGuire und Dowling, 2013a). Die Beantwortung einer solchen Fragestellung wäre u. a. vor dem Hintergrund interessant, wie die Zusammenarbeit von OK-Gruppen in Internetforen gestört werden kann.

Hutchings und Holt (2015) schlagen in diesem Kontext auch weitere Forschungsarbeiten vor, mittels derer Präventions- und Interventionsmethoden erarbeitet werden können, um das Funktionieren von Schwarzmärkten zu untergraben, ohne dabei die Interessen gesetzestreuer Internetnutzer zu sehr zu beeinträchtigen.

7.5 Spezifische Maßnahmen der Jugenddelinquenz

Für Rennie und Shore (2007) stellt jugendliches Hacking lediglich eine Form jugendlicher Abweichung vor, wie sie in UK seit 1997 mit einer ganzen Reihe von Maßnahmen gegen „antisocial behaviour" angegangen wird, in die auch die Eltern eingebunden sind. Rennie und Shore (2007) gehen nicht darauf ein, ob erzieherische Maßnahmen wie die „Acceptable Behaviour Contracts" tatsächlich die erhofften Effekte entfalten, weisen jedoch darauf hin, dass Jugendliche durch die Einflüsse ihrer jeweiligen Peer-Group nicht als autonom handelnde rationale Wesen verstanden werden sollten. Insoweit schlagen sie im Rahmen einer umfassenden Strategie zur Bekämpfung von Hacking nicht nur vor, die elterliche Verantwortung zu stärken, sondern auch den Gruppendruck zu verringern, dem Jugendliche häufig unterliegen, ohne letztgenannten Aspekt allerdings auszuführen.

7.6 Situative Prävention / Verringerung von Tatgelegenheiten

Im Unterschied zu dem sozialen Präventionsansatz, der darauf abzielt, Kriminalität durch verbesserte Erziehung, Wertevermittlung und Bildung sowie die Beseitigung sozialer Mängellagen nachhaltig zu verhindern, geht es dem situativen Ansatz mit einem strikten Fokus auf die Tat einzig darum, die Attraktivität krimineller Handlungen aus Tätersicht zu verringern oder wie Clarke (1997: 2) formuliert hat, „*to make criminal action less attractive to offenders*". Mit dem Fokus auf die Tat ist die situative Prävention formal natürlich kein täterorientierter Ansatz. Wie die nachfolgenden Ausführungen noch zeigen werden, hat der Ansatz mit der Gestaltung von Präventionsmaßnahmen insbesondere über den täterseitigen Mechanismus des rationalen Wahlhandelns (vgl. Kapitel 6.4) allerdings doch einen starken Täterbezug.

Das Rahmengerüst der situativen Prävention besteht aus den vier Komponenten (1) eine theoretische Gründung u. a. in den Theorien des rationalen Wahlhandelns und der Routineaktivitäten (vgl. Kapitel 6.5), (2) einer Standardmethologie, die auf dem Paradigma der Aktionsforschung basiert, (3) einem Satz an Techniken der Tatgelegenheitsreduktion und (4) einer Auswahl guter Praxis einschließlich Studien zur Verdrängung von Kriminalität (vgl. Clarke, 1997).

Die bislang entwickelten 25 Techniken zur Tatgelegenheitsreduktion (http://www.popcenter.org/25techniques/) werden fünf Prinzipien zugeordnet: (1) Tataufwand erhöhen, (2) Entdeckungsrisiko erhöhen, (3) Kriminellen Ertrag mindern, (4) Tatbegünstigende Provokationen reduzieren, (5) Entschuldigungen für kriminelles Verhalten beseitigen. Gerade die ersten drei Prinzipien machen deutlich, dass es um den „rational choice"-Wirkmechanismus geht, in dem opferseitig durch tatgelegenheitsreduzierende Maßnahmen die Kosten für den Täter so hochgeschraubt werden können, dass sich die Tat für diesen nicht mehr „rechnet". Beispiele aus der klassischen Kriminalität sind der Einbau einbruchshemmender Fenster und Türen oder der Einsatz der elektronischen Wegfahrsperre in Kraftfahrzeugen.

Die letzten beiden Prinzipien sind im Zuge der wissenschaftlichen Diskussion der situativen Kriminalprävention in neuerer Zeit entwickelt worden und fokussieren weniger auf rein technische Elemente. Beispielhaft dafür steht das Prinzip der Beseitigung von Entschuldigungsmöglichkeiten, das einen starken Bezug zur Neutralisationstheorie aufweist (vgl. Kapitel 6.3): Die Deutlichmachung von Regeln und Vorschriften (z. B. Aushang

bestimmter Weisungen), die Sensibilisierung durch Erinnerungen (Belehrungen im situativen Kontext) sowie die Erleichterung der Regelbefolgung (z. B. durch Aufstellen von Aktenvernichtern) sind hier beispielhaft zu nennende Mechanismen.

Voraussetzung für die Anwendung situativer Maßnahmen in der Prävention ist allerdings ein fundiertes Wissen über verwendete Modi Operandi bzw. die von Tätern genutzten Skripte. Um das an einem Beispiel zu verdeutlichen: Solange nicht bekannt ist, dass der Zugang zu einer Firmen-IT durch eine bestimmte Form des social engineerings gelungen ist, sind auch keine spezifischen Sensibilisierungs- oder Kontrollmaßnahmen möglich.

Eine Übersicht über situative Präventionsansätze im Bereich Cybercrime haben Hartel et al. (2011) auf der Basis einer umfassenden Literaturanalyse erstellt. Ein Großteil der Techniken setzt beim Opfer an (wie alle Maßnahmen zur Härtung von IT). Spezifisch täterorientiert sind insbesondere Hinweise zum richtigen Verhalten oder auch Awarenessmaßnahmen von Beschäftigten.

Willison (2005) regt an, die 25 Techniken der Tatgelegenheitsreduktion in Ergänzung zu bekannten Skripten zur Begehung von Kriminalität zu nutzen, um in Organisationen (Firmen, Behörden etc.) Maßnahmen der Informationssicherheit zu optimieren.

Nachfolgend werden zwei weitere Beispiele der situativen Prävention genannt, die zudem deutlich machen, wie eng die Prävention mit dem operativen polizeilichen Geschäft verknüpft sein kann. Auf britischer Seite findet sich diesbezüglich der Begriff der taktischen Prävention („tactical prevention“). Gemeint ist damit ein abgestimmtes Vorgehen der Repression (z. B. U-Haft für Haupttäter) und Prävention (wie Gefährderansprachen für eher randständige, unbedeutende Täter).

- Monitoring von / Erschwerter Zugang zu Hacking-Tools

Rennie und Shore (2007) schlagen die Überwachung („monitoring“) der Entwicklung und des Austausches von Hackingwerkzeugen in Chaträumen, auf „Hacking-Warez“-Seiten und auf bekannten Hacking-relevanten Servern vor. Ziel ist die Reduzierung der Verfügbarkeit dieser Werkzeuge. „Skript kiddies“ und andere Möchtegern-Hacker sollen vom Zugang zu diesen Angeboten abgeschreckt, mögliche Flow-Erfahrungen sollen damit unterbunden und Nutzer derartiger Malware-Tools zudem frühzeitig identifiziert werden können. Beispielhaft sei in diesem Kontext auf eine international konzertierte Polizeioperation gegen die Nutzer der BlackShades-Malware im Mai 2014 hingewiesen. Diese Malware, insbesondere das Blackshades Remote Access Tool (RAT) erlaubt Straftätern, Passwörter und sonstige Berechtigungen zu stehlen. Anstelle einzig auf repressive Maßnahmen zu fokussieren, ging die britische Polizei in der Folge gegen alle Käufer dieser Software vor. Abschreckungsmaßnahmen gegen eine Gruppe von etwa 500 eher unbedeutenden Käufern der Software umfassten u. a. warnende Briefe und E-Mails. Darüber hinaus werden Hausbesuche von Mitarbeitern der National Crime Agency (NCA) und der Polizei zu etwa 100 Käufern berichtet (Eurojust, 2015). Über die präventiven Effekte dieser Maßnahme liegen allerdings keine Erkenntnisse vor.

In diesem Kontext sei auf eine Arbeit von Dupont (2013) hingewiesen, nach der „Hackerlehrlinge“ durch Mentoren befähigt werden, bestimmte Werkzeuge zu nutzen. Die Identifizierung und Entfernung der wenigen „technischen Führungskräfte“ – als aus situativer

Sicht „facilitators“ von Cybercrime – wird als verlässlicher Weg angesehen, Hackernetzwerke zu zerschlagen, da diese Schlüsselpersonen nur schwer zu ersetzen sind.

- Warnhinweise

Maimon et al. (2014) haben in zwei quasi-experimentellen Studien die Wirkung von Warnhinweisen („warning banner“) auf Fälle untersucht, in denen sich Personen dadurch unberechtigt Zugang zu fremden Computern verschafft hatten, dass Sicherheitsschwachstellen oder Sicherheitswälle überwunden wurden. Theoretisch fanden die Studien ihre Begründung in den Theorien absoluter und eingeschränkter Abschreckung, nach denen infolge von Sanktionsandrohungen von einer kriminellen Tat völlig abgelassen oder aber zumindest die Häufigkeit und Schwere krimineller Handlungen reduziert wird. Die Studien zeigten im Ergebnis, dass ein in einem erfolgreich attackierten Computer eingespielter Warnhinweis, der explizit Hinweis auf strafrechtliche wie disziplinarrechtliche Konsequenzen aufzeigt, nicht dazu führt, strafbares Handeln unmittelbar (Anm.: innerhalb von 5 Sek.) einzustellen. Das interpretierten die Autoren damit, dass die Täter zunächst ggf. die Früchte ihrer Arbeit ernten wollen. Es fanden sich ebenfalls keine Hinweise darauf, dass Warnhinweise die Zahl an Tatwiederholungen reduzieren. Allerdings führte die Präsentation eines Warnhinweises zu einer signifikanten Reduktion der Dauer der auf einem fremden Computersystem illegal verbrachten Zeit.

7.7 Forschung

Auf die Notwendigkeit weiterer Forschung wird in vielen der analysierten Studien hingewiesen, wobei aus Sicht des Autors bedeutsam erscheint, dass Forschung insbesondere in den Feldern initiiert wird, die einen starken Bezug zur Polizeipraxis haben. Das setzt allerdings voraus, dass die Wissenschaft Interesse an polizeilichen Fragestellungen zeigt und die Polizei auf der anderen Seite Interesse zeigt, das methodische Potenzial zu nutzen, das ihr von wissenschaftlicher Seite zur Verfügung gestellt wird.

Beispielhaft für eine Forschung, die sowohl der Polizei als auch jedem gesetzestreuen Internetnutzer dienen würde, ist hier der bereits zitierte Vorschlag von Hutchings und Holt (2015) zu nennen, die vorschlagen, Präventions- und Interventionsmethoden im Zusammenhang mit Online-Schwarzmärkten zu erforschen.

Darüber hinaus bieten die hier besprochenen Theorien wie auch Interventionen ausreichend Fragestellungen, denen durch eine anwendungsorientierte Forschung auf den Grund gegangen werden könnte. In besonderem Maße sei hier das Themenbündel Kriminalitätsskript / situative Prävention genannt. Mit einer Intensivierung der Forschung und Entwicklung in diesem Bereich sollten sich auch unter Kostenaspekten wirksame Täterinterventionen entwickeln lassen.

8 Ergebnisse

Das Ziel dieser Arbeit lautete, die neuere deutsch- und englischsprachige Literatur zum Thema Cybercrime im engeren Sinne auf täterspezifische Erkenntnisse auszuwerten, unterschiedliche Tätertypen zu beschreiben bzw. vorhandene Tätertypologien zu untersuchen. Dieser Aufgabe wurde insoweit nachgekommen, als mit der Beschreibung einer

Täterphänomenologie zunächst ein Überblick über das Objekt der Typisierung erstellt wurde, bevor in einem zweiten Schritt Tätertypologien selber beschrieben wurden (Teil I). In einem dritten Schritt wurden maßgebliche in der Literatur im Zusammenhang mit dem Hacking erwähnte kriminologische Theorien untersucht, während die Arbeit in einem abschließenden vierten Schritt auf diejenigen Hacker bezogenen Interventions- und Präventionsmaßnahmen Bezug nimmt, die im Rahmen der Literaturerhebung gewonnen wurden (Teil II).

In den letzten 25 Jahren sind Hacker vorrangig nach ihrem Fertigkeitsniveau, dem Zweck bzw. der Motivation ihres Handelns und in neuerer Zeit auch nach ihrer beruflichen Herkunft bzw. ihrem Auftraggeber typisiert worden. Regelmäßig fanden mehrere dieser Faktoren gleichzeitig Berücksichtigung. Hinweise zur methodischen Herangehensweise an die Entwicklung von Tätertypen im Bereich Hacking fanden sich in der Literatur kaum. Das Objekt der Typisierung scheint selbst so faszinierend zu sein, wie ja auch insbesondere frühe Fremd- und Selbstbilder von Hackern belegen, dass kein Raum mehr für Methodisches zu bleiben scheint. Eine tiefergehende methodische Analyse der Typenbildungen von Hackern war insofern im Rahmen dieser Literaturerhebung nicht möglich.

Die Arbeit liefert dennoch nicht nur einen chronologischen Überblick über Typenbildungen bei Hackern, sondern gibt auch einen Überblick in der Breite, der von eher groben Differenzierungen nach dem Fertigkeitsniveau bis hin zu komplexen Typendifferenzierungen insbesondere auch unter motivatorischen Aspekten reicht. In den meisten Typensystemen spielten übrigens beide Aspekte eine Rolle. Neuere Typisierungen referenzieren zudem auf die Herkunft bzw. die institutionelle Zuordnung von Hackern, wie das am Beispiel der Typisierung des niederländischen National Cyber Security Centre deutlich wird. Diese Differenzierung ist auch insofern erwähnenswert, als dass hier versucht wird, basierend auf einem Modell von Hackertypen den Grad der nationalen Gefährdung wiederum als Ausgangspunkt für nationalstaatliche Gegenmaßnahmen zu betrachten.

Aus polizeipraktischer Sicht bedeutsam ist der Hinweis, dass mit dem Grad der Typendifferenzierung auch die Schwierigkeit einer validen Zuordnung steigt. Nun könnte man aus polizeilicher Sicht auch argumentieren, dass die Notwendigkeit einer Differenzierung von „guten“ und „bösen“ Hackern für die Polizei gar nicht besteht, da ein Hacker mit seiner nach objektiven Tatbestandskriterien erfüllten Straftat zunächst erst einmal unabhängig von seiner Motivation, die vielleicht von politisch motivierten Delikten abgesehen häufig gar nicht direkt bzw. verlässlich erkennbar ist, automatisch zum Objekt polizeilichen Handelns wird. So richtig dieses Argument ist, schmälert es auch unter dem Aspekt, knappe polizeiliche Ressourcen möglichst effektiv und effizient einzusetzen, nicht die Bedeutung einer validen Typisierung. Eine Lösung könnte so aussehen, insbesondere die Repression auf die relativ kleine Gruppe kreativer „high sophisticated hacker“ (die in Grafik 1 genannten „versierten Hacker“) als auf die „script-kiddies“ bzw. die Gruppe der angelernten Hacker zu fokussieren, die vorgefertigte Werkzeuge nutzen und ggf. auch mit dem Repertoire sozialer Präventionsansätze erreichbar sind, zu denen u. a. auch die in diesem Bericht aufgeführten Gefährderansprachen zu zählen sind. Die Konzentration der Strafverfolgung auf versierte Hacker dürfte auch deshalb gewinnbringend sein, sind sie doch nicht allein die Entwickler immer neuer Angriffswerkzeuge, sondern zugleich auch wichtige Knoten in der täterbezogenen Zusammenarbeit und wichtige Stützen in der Wissensvermittlung für weniger fachkundige Hacker.

Gerade im Zusammenhang mit den „script-kiddies“ hat Yar (2005a) mit seiner Frage, ob (jugendliches) Hacking nicht schlichtweg ein weiteres Beispiel der Jugenddelinquenz ist, ggf. Hinweise für Handlungsmöglichkeiten gegeben. Auch wenn Hacker mittlerweile zum Teil dem Jugendalter entwachsen sind, muss man auf der Basis der ausgewerteten Literatur hinsichtlich der altersmäßigen Zusammensetzung der Täter von einem hohen Anteil kindlicher, jugendlicher und heranwachsender Täter ausgehen. Die Altersstruktur korreliert mit dem Täteralter im Bereich der Alltagskriminalität. In kriminologischer Hinsicht schlössen sich damit klassische Fragestellungen zur Täterbiografie oder einer möglichen kriminellen Karriere an, die es hier ggf. dank der erworbenen IT-Qualifikationen gar nicht zwingend geben muss. Leider ist die Forschungslage zu derartigen kriminologischen Fragestellungen bislang unzureichend; es bleibt abzuwarten, ob ein derzeit in den Niederlanden durchgeführtes Projekt (vgl. Kranenbarg, 2014) das Dunkel ein wenig aufzuhellen vermag.

In polizeipraktischer Hinsicht ist diese Literaturanalyse in Teil II auch genutzt worden, um Ideen für täterbezogene Interventionen bzw. Präventionsmaßnahmen zu gewinnen. Diese Ideen sind ein Nebenprodukt, ging es in dieser Arbeit doch im Kern um andere Aspekte. Sie sind dennoch in diesen Bericht übernommen worden, um ggf. in der Praxis diskutiert werden zu können. Soweit es um Aspekte der situativen Kriminalprävention geht, bestätigt gerade die kriminologische Betrachtung das große Potenzial, das diesem Ansatz zuzusprechen ist, wie viele Erfolge in eher klassischen Kriminalitätsbereichen belegen. Situative Maßnahmen sind in der Regel nicht geeignet, hochprofessionelle und -motivierte Täter von ihrem Tun abzuhalten. Sie sind jedoch ein wirksames Werkzeug für die Masse opportunistischer Täter bzw. derjenigen Täter, die lediglich Tatgelegenheiten nutzen. Bezogen auf das Thema Hacking wären dies diejenigen – häufig jugendlichen Täter („script-kiddies“) – die vorgefertigte Angriffswerkzeuge nutzen, weil sie selber über zu wenig Wissen und (finanzielle) Möglichkeiten verfügen, komplexe Angriffswerkzeuge zu entwickeln. Situative Ansätze beziehen sich dabei nicht nur auf Maßnahmen der IT-Grundsicherung auf Anwenderseite, sondern lassen sich auch täterseitig einsetzen, um zum Beispiel Neutralisierungsmöglichkeiten zu verhindern.

Im Zuge der Literaturanalyse ist schließlich deutlich geworden, dass die kriminologische Forschung zu täterbezogenen Aspekten im Bereich Cybercrime bislang viele Fragen unbeantwortet lässt. Beginnend beim Thema dieser Arbeit, den Hackertypen, hat sich beispielsweise gezeigt, dass eine auch unter wissenschaftlichen Aspekten tragfähige Typenbildung bislang nicht existiert. Valide Erkenntnisse zu typenspezifischen Anreiz- oder Abschreckungsaspekten existieren bislang ebenfalls nicht. Auffallend sind zudem Forschungsdefizite beispielsweise zur Anwendung von Subkulturtheorien oder zur Fragestellung, ob Hacking in weiten Bereichen nicht lediglich eine weitere Form der Jugenddelinquenz darstellt und welche Konsequenzen möglicherweise daraus zu ziehen sind. Die Frage nach wirksamen Interventions- und Präventionsmethoden ist ebenfalls noch weitgehend unbeantwortet. Beispielhaft dafür steht das unzureichende Wissen über wirksame Mechanismen zur Störung illegaler Märkte im Cyberraum oder über die Wirkung von Gefährderansprachen für die Käufer und potenziellen Nutzer illegaler Hackingtools.

9 Literaturverzeichnis

Aebersold, Peter (2007): Kriminologie 1 – Kriminalitätstheorien (http://ius.unibas.ch/typo3conf/ext/x4eunical/scripts/handleFile.php?file=1383)

Allen, Jonathan; Forrest, Sarah; Levi, Michael; Roy, Hannah und Sutton, Michael (2005): Fraud and Technology Crimes: Findings from the 2002/3 British Crime Survey and 2003 Offending, Crime and Justice Survey. Online Report 34/05. London: Home Office

Akers, Ronald (1990): Rational Choice, Deterrence and Social Learning Theory in Criminology: The Path not taken. In: Journal of Criminal Law and Criminology, 81(3), 653-676

Ann, Christoph (2012): Know-How – Schutz im Arbeitsrecht. 9. ZAAR-Kongress, 04.05.2012 (http://www.zaar.uni-muenchen.de/veranstaltungen/tagungen/archiv/zk09/9_kongress_folien.pdf)

Bachmann, Michael (2010): The Risk Propensity and Rationality of Computer Hackers. In: International Journal of Cyber Criminology, Heft 4 (1&2), 643-656

Bisset, Andy und Shipton, Geraldine (2000): Some human dimensions of computer virus creation and infection. In: International Journal of Human-Computer Studies, 52, 899-913

Bizeul, David (2007): Russian Business Network Study. Online-Ressource

BAE Systems Detica und John Grieve Centre for Policing and Security (Hg.)(2012): Organised Crime in the Digital Age (vmtl. Identisch mit McGuire, Mike (2012): Organised Crime in the Digital Age (John Grieve Centre for Policing and Security, London: Metropolitan University)

Bock, Michael (2015): Kriminologie. 4. Auflage, München: Verlag Franz Vahlen

Bossler, Adam und Holt, Thomas (2009): On-line Activities, Guardianship, and Malware Infection: An Examination of Routine Activities Theory. In: International Journal of Cyber Criminology, Heft 3(1), 400–420

Broadhurst, Roderic; Grabosky, Peter; Alazab, Mamoun; Bouhours, Brigitte; Chon, Steve und Da, Chen (2013): Crime in Cyberspace: Offenders and the Role of Organized Crime Groups. Working Paper, 15.05.2013, Australian National University Cybercrime Observatory

Broadhurst, Roderic; Grabosky, Peter; Alazab, Mamoun und Chon, Steve (2014): Organizations and Cyber crime: An Analysis of the Nature of Groups engaged in Cyber Crime. In: International Journal of Cyber Criminology, Heft 8(1), 1–20 (http://www.cybercrimejournal.com/broadhurstetalijcc2014vol8issue1.pdf)

Brodowski, Dominik und Freiling, Felix (2011): Cyberkriminalität, Computerstrafrecht und die digitale Schattenwirtschaft. In: Schriftenreihe Forschungsforum Öffentliche Sicherheit

Bundeskriminalamt (Hg.)(2012): Polizeiliche Programme zum Umgang mit „Mehrfach- und Intensivtätern“ - Eine Bestandsaufnahme. Wiesbaden: Bundeskriminalamt

Bundeskriminalamt (Hg.)(2014): Cybercrime. Bundeslagebild 2013. Wiesbaden: Bundeskriminalamt

Bundesamt für Sicherheit in der Informationstechnik (Hg.)(2014): Die Lage der IT-Sicherheit in Deutschland 2014. Bonn: BSI

Center for Problem-Oriented Policing (Hg.)(ohne Jahr): Understand the crime from beginning to end (http://www.popcenter.org/learning/60steps/index.cfm?stepNum=35)

Chabinsky, Stephen (2010): The Cyber Threat: Who’s Doing What to Whom? FBI. (http://www.fbi.gov/news/speeches/the-cyber-threat-whos-doing-what-to-whom).

Chandler, Amanda (1996): The changing definition and image of hackers in popular discourse. In: International Journal of the Sociology of Law, 24, 229-251.

Chiesa, Raoul; Ducci, Stefania und Ciappi, Silvio (2009): Profiling Hackers. The Science of Criminal Profiling as Applied to the World of Hacking. Boca Raton: Auerbach Publication

Chon, Steve und Broadhurst, Roderic (2014): Routine Activity Theory and Cybercrime: What about Offender Resources? (http://dx.doi.org/10.2139/ssrn.2379201)

Clarke, Ronald (1997): Introduction . In: Ronald Clarke (Hg.): Situational crime prevention: successful case studies. 2. Auflage, Albany: Harrow and Heston, S. 1-43

Choo, KKR & Smith, RG (2008): Criminal exploitation of online systems by organised crime groups. In: Asian Journal of Criminology 3(1), 37-59.

Cohen, Lawrence und Felson, Marcus (1979): Social Change and Crime Rate Trends: A Routine Activity Approach. In: American Sociological Review 44 (4), 588-608

Cornish, Derek (1994): The procedural analysis of offending and its relevance for situational prevention. In: Ronald Clarke (Hg.): Crime Prevention Studies, Vol. 3, Monsey (NY): Criminal Justice Press, S. 151-196

Cornish, Derek und Clarke, Ronald (1986): The reasoning criminal: Rational Choice Perspectives on Offending. New York: Springer Verlag

Cornish, Derek und Clarke, Ronald (2003): Opportunities, precipitators and criminal decisions: A reply to Wortley s critique of situational crime prevention. In: Martha Smith und Derek Cornish (Hg.) Theory for Situational Crime Prevention. Crime Prevention Studies, 16. Monsey, New York: Criminal Justice Press

Csikszentmihalyi, Mihaly (2007): Flow and Education (http://www.ppc.sas.upenn.edu/csikszentmihalyipowerpoint.pdf)

Csikszentmihalyi, Mihaly; Abuhamdeh, Sami und Nakamura, Jeanne (2005): Flow. In: Andrew Elliot und Carol Dweck (Hg.) Handbook of competence and motivation. S. 598-608, New York, NY, US: Guilford Publications

Danquah, Paul und Longe, Olumide (2011): An Empirical Test of the Space Transition Theory of Cyber Criminality: Investigating Cybercrime Causation Factors in Ghana. In: African Journal of Computing & ICT, Heft 4(2), 37-48.

Décary-Hétu, David und Dupont, Benoit (2012): The social network of hackers. In: Global Crime, iFirst, 1–16 (http://dx.doi.org/10.1080/17440572.2012.702523)

Diedrich, Ingo (2013): Die Kontrolltheorie nach Travis Hirschi – eine Diskussionsvorlage (http://material.or-so.de/Travis_Hirschi_Soziale_Kontrolltheorie.pdf)

Dupont, Benoit (2013): Skills and trust: a tour inside the hard drives of computer hackers. In Carlo Morselli (Hg.): Illicit networks, Routledge: Oxford, 2013, S. 195-217.

Eckert, Roland; Vogelgesang, Waldemar; Wetzstein, Thomas und Winter, Rainer (1991): Auf digitalen Pfaden - Die Kulturen von Hackern, Programmierern, Crackern und Spielern. Opladen: Westdeutscher Verlag

Eifler, Stefanie (2009) Kriminalität im Alltag: Eine handlungstheoretische Analyse von Gelegenheiten, Wiesbaden: VS Verlag für Sozialwissenschaften

Eifler, Stefanie; Schmitt, Stefan, Bentrup, Christina; Hegeler, Malte; Pessara, Isabel; Porr, Christiane; Ratzka, Melanie (2001): Soziale Probleme, Gesundheit und Sozialpolitik. Materialien und Forschungsberichte Nr. 2: Gelegenheitsstrukturen und Kriminalität. Universität Bielefeld

Eurojust (Hg.)(2015): Operation BlackShades. An Evaluation. April 2015 (https://www.gccs2015.com/sites/default/files/documents/Bijlage%202%20-%20Eurojust%20%2810%2004%2015%29%20Blackshades-Case-Evaluation.pdf)

Europarat (Hg.)(2001): Übereinkommen über Computerkriminalität, Budapest, 23.XI.2001

Europol (Hg.)(2015): Exploring tomorrow's Organised Crime. Den Haag: Europol

Feltes, Thomas (2004): Kurzfassung der Studie „Wirksamkeit technischer Einbruchsprävention bei Wohn- und Geschäftsobjekten – Eine Untersuchung unter besonderer Berücksichtigung von aktuellem Täterwissen" (http://www.kriminalpraevention.de/downloads/as/techpraev/Wirksamkeit_Kurzfassung.pdf)

Fisk, Nathan (2006): Social Learning Theory as a Model for Illegitimate Peer-to-Peer Use and the Effects of Implementing a Legal Music Downloading Service on Peer-to-Peer Music Piracy, A Thesis Presented to The Faculty of the Department of Communication (September 14, 2006) (http://scholarworks.rit.edu/cgi/viewcontent.cgi?article=5134&context=theses)

Fortinet (Hg.)(2013): Cybercriminals Today Mirror Legitimate Business Processes. Sunnyvale: Fortinet Inc.

Foster, Peter (2015): Anonymous hackers turn fire on global paedophile menace. In: The Telegraph, 23.01.2015 (http://www.telegraph.co.uk/news/worldnews/northamerica/usa/11363303/Anonymous-hackers-turn-fire-on-global-paedophile-menace.html)

Fötinger, Christian und Ziegler, Wolfgang (2004): Understanding a hacker's mind – A psychological insight into the hijacking of identities. White Paper by the Danube-University Krems, Austria.

Füllgraf, Wendy (2015): Hacktivisten. Abschlussbericht zum Projektteil der Hellfeldbeforschung. Wiesbaden: Bundeskriminalamt [aktualisierte Version vom 20.02.2015]

Furnell, Steven (2002). Cybercrime: Vandalizing the Information Society . London: Addison-Wesley

Fritsche, Klaus-Dieter (2014): Eröffnungsansprache: Cyberkriminalität - globale Herausforderungen weltweiter Netzwerke. In: Bundeskriminalamt (Hg.): Cybercrime - Bedrohung, Intervention, Abwehr. Wiesbaden: Bundeskriminalamt, S. 9–20

Gaycken, Sandro (2014): Cyberterrorismus, Cyberspionage und Cyberwar - eine aktuelle Bedrohungseinschätzung aus Sicht der Wissenschaft. In: Bundeskriminalamt (Hg.): Cybercrime - Bedrohung, Intervention, Abwehr. Wiesbaden: Bundeskriminalamt, S. 26-38

Geschonneck, Alexander; Fritzsche, Thomas und Weiand, Klara (2013): E-Crime. Computerkriminalität in der deutschen Wirtschaft mit Kennzahlen für Österreich und Schweiz. Berlin: KPMG

Geschonneck, Alexander; Fritzsche, Thomas; Weiand, Klara und Scheben, Marc (2015): E-Crime. Computerkriminalität in der deutschen Wirtschaft 2015. Berlin: KPMG

Gibbs, Jack (1975): Crime, Punishment and Deterrence. New York: Elsevier Scientific

Glenny, Misha (2012): CyberCrime: Kriminalität und Krieg im digitalen Zeitalter. München.

Gnörlich, Carsten (2011): Forum Offene Wissenschaft. Verletzlichkeit der Informationssysteme. Bielefeld. Präsentation.

Gordon, Sarah (2000): Virus Writers: The End of The Innocence? (http://vxheaven.org/lib/asg12.html#p3)

Gordon, Sarah und Ma, Qingxiong (2003): Convergence of Virus Writers and Hackers: Fact or Fantasy? White Paper, Symantec Security Response

Grabosky, Peter (2000): Computer Crime: A Criminological Overview (http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.3.4660&rep=rep1&type=pdf)

Gu, Lion (2013): Beyond Online Gaming Cybercrime: Revisiting the Chinese Underground Market. Irving: Trend Micro Security Intelligence

Gyapjas, Anne (2015): Frauen im Chaos Computer Club. Das Vorurteil vom krassen Hacker ist passé. In: Frankfurter Allgemeine Zeitung vom 13.08.2015.

Hafner, Katie und Markoff, John (1992): Cyberpunk: Outlaws and Hackers on the Computer Frontier. New York: A Touchstone Book

Hartel, Pieter (2014): Situative Prävention von Cybercrime: ein chancenreicher Bekämpfungsansatz. In: Bundeskriminalamt (Hg.): Cybercrime - Bedrohung, Intervention, Abwehr. Wiesbaden: Bundeskriminalamt, S. 96-104

Hartel, Pieter; Junger, Mariann und Wieringa Roel (2011): Cyber-crime Science = Crime Science + Information Security (http://eprints.eemcs.utwente.nl/18500/03/0_19_CCS.pdf)

Heise-online (Hg.)(2014): Europol: Nur 100 Malware-Programmierer weltweit. Meldung vom 11.10.2014 (http://www.heise.de/newsticker/meldung/Europol-Nur-100-Malware-Programmierer-weltweit-2415556.html)

Heise-online (Hg.)(2015): Exploit-Kit Rig: Verbrechen lohnt sich wieder. Meldung vom 06.08.2015 (http://www.heise.de/newsticker/meldung/Exploit-Kit-Rig-Verbrechen-lohnt-sich-wieder-2772951.html)

Held, Warren (2012). Hacktivism - an Analysis of the Motive to Disseminate Confidential Information. (https://digital.library.txstate.edu/handle/10877/4381)

Herbst, Barbara (2013): Hacktivisten. Eine literaturbasierte Sekundäranalyse. BKA Wiesbaden (unveröffentlicht)

Hess, Henner und Scherer, Sebastian (2003): Theorie der Kriminalität. In: Oberwittler und Karstedt (Hg.), Soziologie der Kriminalität, Sonderheft 43, 69-92

Hollinger, Richard (1988): Computer hackers follow a guttman-like progression. Social Sciences Review, 72, 199-200.

Holt, Thomas (2007): Subcultural evolution? Examining the influence of on- and off-line experiences on deviant subcultures. In: Deviant Behavior, 28: 171-198.

Holt, Thomas (2010): Examining the role of technology in the formation of deviant subcultures. In: T. Holt (ed.), Cybercrime and criminological theory, 2013, S. 213-224.

Holt, Thomas (2013): Examining the forces shaping cybercrime markets online. In: Social Science Computer Review, 31, 165-177.

Holt, Thomas (2014): Considering the Hacker Subculture. In: ACJS Today, Volume XXXVIIII, Issue 1, January 2014 (http://www.acjs.org/uploads/file/ACJS_Today_January_2014.pdf)

Holt, Thomas und Bossler, Adam (2009): Examining the Applicability of Lifestyle-Routine Activities Theory for Cybercrime Victimization. In: T. Holt (ed.), Cybercrime and criminological theory, 2013, S. 75-88

Holt, Thomas und Kilger, Max (2012): Know Your Enemy: The Social Dynamics of Hacking. The Honeynet Project (http:/ / www.honeynet.org)

Holt, Thomas; Kilger, Max; Strumsky, Deborah und Smirnova, Olga (2009): Identifying, Exploring, and Predicting Threats in the Russian Hacker Community. Presented at the Defcon 17 Convention (https://www.defcon.org/html/links/dc-archives/dc-17-archive.html)

Holt, Thomes; Soles, Joshua und Leslie, Ludmilla (2008): Characterizing malware writers and computer attackers in their own words. 3. International Conference on Information Warfare and Security, 24. – 25. April 2008 in Omaha, Nebraska

Holt, Thomas; Strumsky, Deborah; Smirnova, Olga und Kilger, Max (2012): Examining the Social Networks of Malware Writers and Hackers. In: International Journal of Cyber Criminology, Heft 6(1), 891–903

Hutchings, Alice (2014): Crime from the keyboard: organised cybercrime, co-offending, initiation and knowledge transmission. In: Crime, Law and Social Change, 62 (1), 1-20, http://link.springer.com/article/10.1007%2Fs10611-014-9520-z

Hutchings, Alice und Holt, Thomas (2015): A crime script analysis of the online stolen data market. In: British Journal of Criminology, 55 (3), 596-614

IBM (Hg.)(2015): IBM 2015 Cyber Security Intelligence Index. Analysis of cyber attack and incident data from IBM's worldwide security services operations (http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=WH&infotype=SA&htmlfid=SEW03073USEN&attachment=SEW03073USEN.PDF)

Infosec Institute (Hg.)(2015): Hacking communities in the Deep Web. Posted in General Security, Hacking on May 15, 2015 (http://resources.infosecinstitute.com/hacking-communities-in-the-deep-web/)

Jaishankar, K. (2008). Space Transition Theory of Cyber Crimes. In: F. Schmalleger & M. Pittaro (Hg.), Crimes of the Internet. Upper Saddle River, NJ: Prentice Hall, S. 281-283

Jordan, Tim und Taylor, Paul (1998): A sociology of hackers. In: The Sociological Review, 46, 757-780.

Jordan, Tim und Taylor, Paul (2004): Hacktivism and cyberwars: rebels with a cause? London, New York.

Kaiser, Günther (1996): Kriminologie. 3. Auflage, Heidelberg: C.F. Müller Verlag.

Kaspersky Lab & Interpol (Hg.)(2014): Mobile Cyber Threats. (http://25zbkz3k00wn2tp5092n6di7b5k.wpengine.netdna-cdn.com/files/2014/10/report_mobile_cyberthreats_web.pdf)

Kempa, Darius (2006): Angriffe auf Netze und Systeme. Hackerkultur zwischen gesellschaftlicher Anerkennung und Kriminalisierung. Universität Hamburg (http://ediss.sub.uni-hamburg.de/volltexte/2006/3025/pdf/Dissertation.pdf)

Killias, Martin, Scheidegger, David und Nordenson, Peter (2009): Effects of increasing the certainty of punishment: a field experiment on public transportation. In: European Journal of Crimiology. 6 (5), 387-400

Kilger, M., Stutzman, J ., & Arkin, O. (2004). Profiling. In: The Honeynet Project (2. Ausgabe.), Know your enemy. Addison Wesley Professional.

Kirwan, Granine; Power, Andrew (2013): Cybercrime: the psychology of online offenders. Cambridge: University Printing House

Kluge, Susann (2000): Empirisch begründete Typenbildung in der qualitativen Sozialforschung. In: Forum Qualitative Sozialforschung / Forum: Qualitative Social Research, 1(1), Art. 14 (http://www.qualitative-research.net/index.php/fqs/article/viewFile/1124/2498)

Kranenbarg, Marleen (2014): Cybercrime offenders: A distinct offender group? Abstract Cybercrime Conference Understanding patterns and developments in cybercrime: Social science perspectives. 06.11.2014, Rotterdam (http://www.esl.eur.nl/fileadmin/ASSETS/frg/pub/criminologie/Cybercrime/Cybercrime

_offenders_a_distinct_offender_group.pdf)

Krebs, Brian (2003): Hackers to face tougher sentences. In: Washington Post Newsweek Interactive v. 02.10.2003 (https://citizenlab.org/2003/10/hackers-to-face-tougher-sentences/)

Krömer, Jan ; Sen, William (2011): Hackerkultur und Raubkopierer : eine wissenschaftliche Reise durch zwei Subkulturen, 2. Aufl., Social-Media-Verl. Köln.

Kshetri, Nir (2010): The Global Cybercrime Industry. Economic, Institutional and Strategic Perspectives. Heidelberg: Springer

Landreth, B. (1985). Out of the inner circle. Redmomd: Microsoft Books.

Leukfeldt, Rutger; Veenstra, Sander und Stol, Wouter (2013): High Volume Cyber Crime and the Organization of the Police: The results of two empirical studies in the Netherlands. In: International Journal of Cyber Criminology, Heft 7(1), 1–17 (http://www.cybercrimejournal.com/Leukfeldtetal2013janijcc.pdf)

Levy, Steven (1984): Hackers: Heroes of the Computer Revolution. Penguin Books: New York

Li, Xingan (2008): The Criminal Phenomenon on the Internet. In: Hallmarks of Criminals and Victims Revisited through Typical Cases Prosecuted. University of Ottawa Law & Technology Journal , 5(1-2),125-140

Loper, Kall (2009): Digital Crime: Hackers, Part 2. Law Enforcement Training Network.

Lösel, Friedrich und Schmucker, Martin (2008): Kriminalitätstheorien [Theories of crime]. In Volbert und Steller (Hg.): Handbuch Rechtspsychologie [Handbook of psychology and law], S. 15-27), Göttingen: Hogrefe.

Lowman, Sarah (2010): Criminology of Computer Crime. (http://lowmanio.co.uk/share/TheCriminologyofComputerCrime.pdf)

Lu, Chi; Jen, WenYuan; Chang, Weiping und Chou, Shihchieh (2006): Cybercrime & Cybercriminals. In: Journal of Computers, 1(6), S. 1-10

Lusthaus, Jonathan (2013): How organised is organised cyber crime? In: Global Crime, 14(1), 52–60

Maimon, David; Alper, Mariel; Sobesto, Bertrand und Cukier, Michel (2014): Restrictive deterrent effects of a warning banner in an attacked computer system. In: Criminology, 52 (1), 33-59.

Marcum, Catherine; Higgins, George und Tewksbury, Richard (2012): Incarceration or community placement: examining the sentences of cybercriminals. In: Criminal Justice Studies, 25 (1), 33-40

McCoy, Damon; Pitsillidis, Andreas; Jordan, Grant; Weaver, Nicholas; Kreibich, Christian; Krebs, Brian; Voelker, Geoffrey; Savage, Stefan und Levchenko, Kirill (2012): PharmaLeaks: Understanding the Business of Online Pharmaceutical Affiliate Programs. In: Proceedings of the 21st USENIX conference on Security symposium

McGuire, Mike; Dowling, Samantha (2013a): Cyber crime: A review of the evidence. Research Report 75. Chapter 1: Cyber-dependent crimes. London: Home Office

McGuire, Mike; Dowling, Samantha (2013b): Cyber crime: A review of the evidence. Research Report 75. Chapter 2: Cyber-enabled crimes - fraud and theft. London: Home Office

Meier, Bernd-Dieter (2012): Sicherheit im Internet. Neue Herausforderungen für Kriminologie und Kriminalpolitik. In MschrKrim, 95 (3), 184-204

Mercês, Fernando (2014): The Brazilian Underground Market: The Market for Cybercriminal Wannabes? Irving: Trend Micro Security Intelligence

Mizrach, Steven (1997?): Is There a Hacker Ethic for the 90s Hackers? (http://www2.fiu.edu/~mizrachs/hackethic.html)

Moore, Robert (2011): Digital File Sharing: An Examination of Neutralization and Rationalization Techniques Employed by Digital File Sharers. In: K. Jaishankar (ed.), Cyber Criminology. Exploring Internet Crimes and Criminal Behaviour, Boca Raton: Taylor & Francis, S. 209-226.

Morris, Robert (2010): Identity Thieves and Levels of Sophistication: Findings from a National Probability Sample of American Newspaper Articles 1995-2005. In: Deviant Behavior 31 (2), 184-207

National Cyber Security Centre (Hg.)(2012): Cyber Security Assessment Netherlands. CSBN-2. Den Haag: Ministry of Security and Justice (https://english.nctv.nl/publications-products/Cyber_Security_Assessment_Netherlands/)

National Cyber Security Centre (Hg.)(2013): Cyber Security Assessment Netherlands. CSAN-3. Den Haag: Ministry of Security and Justice

National Cyber Security Centre (Hg.)(2014): Cyber Security Assessment Netherlands. CSAN-4. Den Haag: Ministry of Security and Justice (https://www.ncsc.nl/binaries/content/documents/ncsc-en/current-topics/news/cyber-securty-assessment-netherlands-4-cybercrime-and-digital-espionage-remain-the-biggest-threat/1/CSAN%2B4.pdf)

Neubacher, Frank (2011): Kriminologie. Baden-Baden: Nomos Verlagsgesellschaft

Newman, Graeme und McNally, Megan (2005): Identity Theft Literature Review. (https://www.ncjrs.gov/pdffiles1/nij/grants/210459.pdf)

Nhan, Johnny und Bachmann, Michael (2015): Developments in Cyber Criminology. In: Okada und Maguire (Hg.): Critical Issues in Crime and Justice. Thought, Policy, and Practice. Thousand Oaks: Sage.

Olson, Parmy (2012): Inside Anonymous. Aus dem Innenleben des globalen Cyber-Aufstands. München: Redline-Verlag

Parker, Donn (1998). Fighting computer crime: A new framework for protecting information. New York: John Wiley & Sons, Inc.

Pfeiffer, Peter und Telser, Christine (2003): Cybercrime und Persönlichkeit: Psychologische Hintergründe zur Tätertypologie bei Internet-Kriminalität. In: Stein, Frank (Hg.):

Grundlagen der Polizeipsychologie. 2. Auflage, Hogrefe, Göttingen, S. 155-163

Picko, Helmut und Hahn, Alexander (2007): Neue Wege in der Kontrolle der Internetkriminalität - die täterorientierte Prävention im Phänomen Hacking. In: Deutsches Polizeiblatt, Heft 5, 31-34.

Randazzo, Marisa; Keeney, Michelle; Cappell, Dawn und Moore, Andrew (2004): Insider threat study: Illicit cyber activity in the banking and finance sector: Carnegie Mellon Software Engineering Institute (http://www.secretservice.gov/ntac/its_report_040820.pdf)

Rennie, Lara und Shore, Malcolm (2007): An Advanced Model of Hacking. In: Security Journal, Heft 20, 236-251

Rheinberg, Falko und Tramp, Nadine (2006): Anreizanalyse intensiver Freizeitnutzung von Computern: Hacker, Cracker und zweckorientierte Nutzer. In: Zeitschrift für Psychologie 214 (2) S. 97-107

Robertz, Frank J.; Rüdiger, Thomas Gabriel (2012): Die Hacktivisten von Anonymous; Der schmale Grat zwischen guter Absichtund Selbstjustiz. In: Kriminalistik, 2012 (2), 79-84.

Rogers, Marcus (2000) A new hacker taxonomy. (http://homes.cerias.purdue.edu/~mkr/hacker.doc)

Rogers, Marcus (2001) Psychological Theories of Crime and "Hacking" (http://homes.cerias.purdue.edu/~mkr/crime.doc)

Rogers, Marcus (2005): The development of a meaningful hacker taxonomy: A two dimensional approach. CERIAS Tech Report 2005-43 (http://www.cerias.purdue.edu/apps/reports_and_papers/view/2845)

Rumpf, Hans-Jürgen; Meyer, Christian; Kreuzer, Anja und John, Ulrich (2011): Prävalenz der Internetabhängigkeit (PINTA). Bericht an das Bundesministerium für Gesundheit (http://www.drogenbeauftragte.de/fileadmin/dateien-dba/DrogenundSucht/Computerspiele_Internetsucht/Downloads/PINTA-Bericht-Endfassung_280611.pdf)

Samuel, Alexandra (2004): Hacktivism and the Future of Political Participation. (http://www.alexandrasamuel.com/dissertation/pdfs/Samuel-Hacktivism-entire.pdf)

Sandee, Michael (2015): Game Over ZeuS. Backgrounds on the Badguys and the Backends. Fox-IT-Whitepaper

Schell, Bernadette und Dodge, John (2002): The Hacking of America: Who's Doing it, Why , and How. Westport, CT: Quorum Books

Schneier, Bruce (2003): Airplane Hackers. In: Schneier on Security (https://www.schneier.com/essays/archives/2003/11/airplane_hackers.html)

Sharma, Raghav (2012): Peeping into a Hacker's Mind: Can Criminological Theories Explain Hacking? Verfügbar über: Social Science Research Network (http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1000446)

Shinder, Debra (2002): Scene of the Cybercrime - Computer Forensics Handbook. Rockland (MA): Syngress Publishing

Skinner, William und Fream, Anne (1997): A Social Learning Theory Analysis of Computer Crime among College Students. In: Journal of Research in Crime and Delinquency, 34 (4), 495-518

Steinmetz, Kevin (2015): Craft(y)ness: An Ethnographic Study of Hacking. In: British Journal of Criminology, 55 (1), 125-145

Sykes, Gresham und Matza, David (1957): Techniques of Neutralization: A Theory of Delinquancy. In: American Sociological Review 22 (6), 664-670.

Taylor, Paul (1999): Hackers - Crime and the Digital Sublime. New York: Routledge

Taylor, Paul (2000): Hackers – cyberpunks or microserfs? In: Douglas Thomas und Brian Loader (Hg.): Cybercrime: Law Enforcement, Security and Surveillance in the Information Age, London: Routledge.

Tompson, Lisa und Chainey, Spencer (2011): Profiling illegal waste activity: Using crime scripts as a data collection and analytical strategy. In: European Journal of Criminal Policy and Research, 17(3), 179-201.

Turgeman-Goldschmidt, Orly (2011): Identity Construction Among Hackers. In: Jaishankar, K. (Hg.): Cyber Criminology. Exploring Internet Crimes and Criminal Behavior. Boca Raton: Taylor & Francis, S. 31-51

United Nations Office on Drugs and Crime (Hg.)(2013): Comprehensive Study on Cybercrime. Draft, February 2013. New York: United Nations

Van Beveren, John (2001): A conceptual model for hacker development and motivations [Online]. Journal of E-Business. (http://www.dvara.net/HK//beveren.pdf)

Veil, Katja (2008): Sicherheit im Wohnquartier und Stadtplanung Herausforderungen und Perspektiven am Beispiel ethnischer Minderheiten in Großbritannien. Münster: LIT-Verlag

Verizon (Hg.)(2015): Data Breach Investigations Report.

Vick, Jens; Roters, Franz (2003): Account-Missbrauch im Internet. Ein Sammelverfahren mit anschließender kriminologischer Auswertung. Wiesbaden: Bundeskriminalamt

Voiskounsky, Alexander und Smyslova, Olga (2003): Flow-based model of computer hackers' motivation. In: CyberPsychology and Behavior, 6(2), 171-180.

Von Liszt, Franz (1905): Der Zweckgedanke im Strafrecht (1882), In: ders., Strafrechliche Aufsätze und Vorträge, Bd. 1, 1905, S. 126 ff.

Wada, Friday; Longe, Olumide und Danquah, Paul (2012): Action Speaks Louder than Words - Understanding Cyber Criminal Behavior Using Criminological Theories. In: Journal of Internet Banking and Commerce, April 2012, Heft 17(1) (http://www.arraydev.com/commerce/jibc/2012-04/Wada%20&%20Longe%20&%20Paul%20acceptedv02.pdf)

Weisburd, David; Waring, Elin und Chayet, Ellen (2001): White-collar crime and criminal careers. Cambridge: Cambridge University Press

Wible, Brent (2003): A site where hackers are welcome: Using hack-in contests to shape preferences and deter computer crime. In: The Yale Law Journal, 112 (6) 1577-1623

Wikipedia (2014): Tätertypologie (vgl. http://de.wikipedia.org/wiki/T%C3%A4tertypologie)

Willison, Robert (2005) Considering the Offender - Addressing the Procedural Stages of Computer Crime in an Organisational Context. Working Paper (http://openarchive.cbs.dk/handle/10398/6462)

Wilson, Debbie; Patterson, Alison; Powell, Gemma und Hembury, Rachelle (2006): Fraud and technology crimes: Findings from the 2003/04 British Crime Survey, the 2004 Offending, Crime and Justice Survey and administrative sources. Online Report 09/06, London: Home Office.

Witte, Randy (2013): Hacker im Wandel der Zeit: Über die differenzierte Verwendung des Hackerbegriffes. Hamburg: Bachelor + Master Publishing

Woo, Hyung-Jin (2003): The hacker mentality: Exploring the relationship between psychological variables and hacking activities. Dissertation Abstract. (https://getd.libs.uga.edu/pdfs/woo_hyung-jin_200305_phd.pdf)

Yar, Majid (2005a): Computer hacking: Just another case of juvenile delinquency? In: Howard Journal of Criminal Justice, 44, 387-399.

Yar, Majid (2005b): An Assessment in light of routine activity theory. In: T. Holt (Hg.), Cybercrime and criminological theory, 2013, 65-74

Yar, Majid (2005c): The novelty of 'cybercrime': An assessment in light of routine activity theory. In: European Journal of Criminology, 2(4),407-427.

Yip, Michael; Webber, Craig und Shadbolt, Nigel (2013): Trust among Cybercriminals? Carding Forums, Uncertainty and Implications for Policing. In: Policing and Society: An International Journal of Research and Policy, 23, (4), 516-539.

Young, Randall; Zhang, Lixuan und Prybutok, Victor (2007): Hacking into the minds of hackers. In: Informations Systems Management, 24, 281-287

Internet-Quellen:

25 Techniken zur Tatgelegenheitsreduktion: http://www.popcenter.org/25techniques/

Computer Science Degree (Hg.)(2013): 10 Notorious Female Hackers (http://www.computersciencedegreehub.com/10-notorious-female-hackers/)

Federal Trade Commission (Hg.): Consumer Information. Identity Theft (http://www.consumer.ftc.gov/features/feature-0014-identity-theft)

Golem.de: Tox - Kostenloser digitaler Erpressungsdienst (http://www.golem.de/news/tox-kostenloser-digitaler-erpressungsdienst-1505-114301.html)

Hacker Profiling Project (HPP): http://www.isecom.org/home.html

Jargon File, Vers. 2.1.1 [draft], 12 Juni 1990: http://www.catb.org/jargon/oldversions/jarg211.txt

The Hacker's Manifesto: http://www.usc.edu/~douglast/202/lecture23/manifesto.html

Wikipedia:

- Flow (Psychologie): https://de.wikipedia.org/wiki/Flow_%28Psychologie%29
- Hacker: http://de.wikipedia.org/wiki/Hacker
- Soziale Netzwerkanalyse: https://de.wikipedia.org/wiki/Soziale_Netzwerkanalyse

ZDNet: Cyber-Angriffe auf Unternehmen werden 2015 zum „Massenphänomen" (http://www.zdnet.de/88218091/cyber-angriffe-auf-unternehmen-werden-2015-zum-massenphaenomen/