Bundeskriminalamt

HACKTIVISTEN

Abschlussbericht zum Projektteil der Hellfeldbeforschung

Bundeskriminalamt
Kriminalistisches Institut
Forschungs- und Beratungsstelle Cybercrime KI 16

BKA

Wendy Füllgraf
KI 16 Forschungs- und Beratungsstelle Cybercrime
Bundeskriminalamt
65173 Wiesbaden
ki16@bka.bund.de

0 Abbildungsverzeichnis IV

1 Einleitung 1

2 Projektbeschreibung 3

2.1 Hintergrund 3

2.2 Projektziele 3

3 Methoden 5

3.1 Angemessenheit der Methode am Forschungsgegenstand 5

3.2 Sekundäranalyse 6
3.2.1 Materialerhebung 6
3.2.2 Auswertung 8

3.3 Fallanalyse 9
3.3.1 Datenerhebung 9
3.3.2 Auswertung 12

3.4 Expertenarbeitstreffen 13
3.4.1 Inhalte und Ablauf 13
3.4.2 Phänomenbezug der Teilnehmer 15
3.4.3 Arbeitsgruppen 15

3.5 Selektionseffekte und Verzerrfaktoren 18

4 Ergebnisse 20

4.1 Begriffliche Abgrenzung 20
4.1.1 Hacktivismus vs. Hacking 20
4.1.2 Cyberterrorismus 22
4.1.3 Internetaktivismus 23
4.1.4 Cyberkriminelle jenseits von politischen oder sozialen Motiven 24
4.1.5 Cyberkriegsführung 25

4.2 Phänomenologie 26
4.2.1 Modi operandi 26
4.2.2 Infrastruktur 33
4.2.3 Szene 34
4.2.4 Geschädigte und Schäden 39
4.2.5 Einzeltäter oder Gruppierungen 46
4.2.6 Soziodemographische und -ökonomische Tätermerkmale 49
4.2.7 Motive und Zielrichtungen 54

4.3 Zusammenfassung und Zusammenhänge 58

5 Bewertung und Diskussion der Ergebnisse 69

5.1 Umsetzung der Projektziele 69

5.2 Expertenarbeitstreffen 70
5.2.1 Praxisbewertung der Ergebnisse 70
5.2.2 Erweiterte Betrachtung des Phänomens 72
5.2.3 Risikofaktoren im Umgang mit Hacktivismus und Cybercrime allgemein 78

6 Fazit 80

7 Literaturverzeichnis 82

8 Anlagen V

0 Abbildungsverzeichnis

Abbildung 1: Propaganda. 1
Abbildung 2: In der Sekundäranalyse ausgewertete Quellen. 8
Abbildung 3: Analytische Definition im Anschreiben. 10
Abbildung 4: Zulieferungen aus den Bundesländern. 11
Abbildung 5: Zulieferungen der Staatsanwaltschaften. 11
Abbildung 6: Zulieferungen der Polizeien. 12
Abbildung 7: Auszug aus dem Erhebungsbogen. 13
Abbildung 8: Vorgehensweisen. Held, W.V. (2012). Hacktivism: an Analysis of the Motive to Disseminate Confidential Information. – Vorgehensweisen 31
Abbildung 9: Darstellung der Vorgehensweise bei 78 Fällen. 32
Abbildung 10: Darstellung des angewendeten Straftatbestands bei 78 Fällen. 33
Abbildung 11: Von Anonymous genutzte Grafik. 36
Abbildung 12: Hacktivistische Zielrichtungen. Held, W.V. (2012). Hacktivism: an Analysis of the Motive to Disseminate Confidential Information. 40
Abbildung 13: Geschädigte in 78 Fällen. 44
Abbildung 14: Schaden in 17 Fällen; 61 Fälle ohne Angaben. 46
Abbildung 15: Vom Täter hinterlassene Bekennung zur Tat. 47
Abbildung 16: Hacktivistische Gruppierungen mit Fallzahl. 48
Abbildung 17: Altersverteilung bei 37 Beschuldigten. 50
Abbildung 18: Geschlechterverteilung bei 37 Beschuldigten. 51
Abbildung 19: Staatszugehörigkeit bei 37 Beschuldigten. 52
Abbildung 20 Bildungsstatus bei 37 Beschuldigten. 53
Abbildung 21: Beschäftigungsstatus bei 37 Beschuldigten. 54
Abbildung 22: Motivlage in 78 Fällen. 57
Abbildung 23: Politischer Tathintergrund in 78 Fällen. 58
Abbildung 24: Vorgehensweise bezogen auf Geschädigte in 78 Fällen. 60
Abbildung 25: Schaden nach Vorgehensweise in 17 Fällen; 61 Fälle ohne Angaben. 61
Abbildung 26: Schaden bezogen auf Geschädigte in 17 Fällen; 61 Fälle ohne Angaben. 61
Abbildung 27: Bekennung zur Tat bezogen auf Vorgehensweise in 78 Fällen. 62
Abbildung 28: Hacktivistische Gruppierungen mit Angriffszielen. 63
Abbildung 29: Geschlechterverteilung nach Alter bei 37 Beschuldigten. 66
Abbildung 30: Tatmotiv bezogen auf Geschädigte in 78 Fällen. 67
Abbildung 31: Vorgehensweise bezogen auf Motiv in 78 Fällen. 67
Abbildung 32: Bekennung zur Tat bezogen auf Tatmotiv in 78 Fällen. 68

1 Einleitung

Abbildung 1: Propaganda.

"*There may be times when we are powerless to prevent injustice, but there must never be a time when we fail to protest*." Elie Wiesel[1]

Hacktivismus ist ein neues Phänomen, hervorgebracht durch die globale informations- und kommunikationstechnische Vernetzung. Ohne IuK-Technologien, ohne soziale Medien und ohne das Internet gäbe es keinen Hacktivismus, der als eines von vielen Cybercrime-Phänomenen letztlich nichts anderes als die digitalisierte Form von Aktivismus ist.

Fundierte Erkenntnisse zu diesem Phänomen gibt es kaum. Literatur und Studien zum Hacktivismus sind rar. In Medien, Politik und Gesellschaft herrscht Begriffsverwirrung, Hacktivismus wird hier häufig mit Cyberterrorismus verwechselt oder per se mit profitorientierten Cyberkriminellen gleichgesetzt. Immer wieder wird von der Gefahr drohender Angriffe auf kritische Infrastrukturen gesprochen, die auch oder vor allem von Hacktivisten befürchtet werden.

Um die Szene der Hacktivisten, ihr Vorgehen und das Gefährdungspotenzial hacktivistischer Aktionen genauer beschreiben zu können und von verwandten Cybercrime-Phänomenen wie z. B. denen des Hackings und des Cyberterrorismus abzugrenzen, wurde das nun vorliegende Projekt mit der Fokussierung auf das Hellfeld konzipiert (Kapitel 2).

Mittels Erhebung vorhandener Erkenntnisse zu Hacktivismus und Hacktivisten aus Fachliteratur und Studien wurde eine erste fundierte Grundlage geschaffen (Kapitel 3.2), die durch die Auswertung registrierter deutscher hacktivistischer Fälle erweitert wurde (Kapitel

[1] Die hacktivistische Gruppierung Anonymous nutzt dieses Zitat von Wiesel für die eigene Propaganda. http://www.anonymousartofrevolution.com/2012/09/there-may-be-times-when-we-are.html

3.3). Diese Erkenntnisse aus dem Hellfeld wurden Experten aus den Bereichen des polizeilichen Staatsschutzes, der Strafverfolgung und der Forschung vorgestellt (Kapitel 3.4). Hacktivisten nutzen ähnliche Vorgehensweisen wie andere Cyberkriminelle – wie z. B. DDoS-Angriffe, Web-Defacements, Ausspähen von Daten etc. – jedoch mit einer anderer Zielrichtung: So agieren Hacktivisten niemals profitorientiert, sondern um sich für ideologische Zwecke und Prinzipien einzusetzen und Sympathisanten zu mobilisieren. Dass dabei dennoch materieller Schaden entstehen kann, zeigen die Beispiele (Kapitel 4).

Es konnten eine erste fundierte Erkenntnisbasis zum Phänomen Hacktivismus und eine klare begriffliche und inhaltliche Abgrenzung zu anderen Cybercrime-Phänomenen geschaffen werden (Kapitel 4). Aufgrund fehlender Informationen zu Tätern und/oder Schäden in den registrierten Fällen konnte der Projektteil zum Hellfeld jedoch nicht alle Ziele vollständig umsetzen. Durch die Bewertung der gewonnenen Erkenntnisse zum Phänomen durch die Experten konnten die Ergebnisse entsprechend ihrer Relevanz in die repressive, präventive und akademische Praxis eingeordnet werden (Kapitel 5).

Um die bisherige aus dem Hellfeld gewonnene Erkenntnisbasis zu erweitern und zu vervollständigen, sollen in einem anschließenden Projektteil „Dunkelfeld“ mittels verschiedener Methoden weitere Erkenntnisse zu den Aspekten des Hacktivismus gewonnen werden, die bislang zu sehr im Dunkeln geblieben sind, weil Fälle beispielsweise nicht zur Anzeige gebracht und (polizeilich) registriert wurden (Kapitel 6).

2 Projektbeschreibung

2.1 Hintergrund

Die vorliegende Hellfeld-Studie im Rahmen des Projektes „Hacktivisten“ wurde im Januar 2013 begonnen und im Februar 2014 abgeschlossen. Das um eine Dunkelfelduntersuchung weitergeführte Projekt wird voraussichtlich im April 2015 abgeschlossen sein. Ziel des Projekts ist es, vor dem Hintergrund der zunehmenden medialen Präsenz von hacktivistischen Aktivitäten und Taten in der Vergangenheit und einem vorherrschenden uneinheitlichen Verständnis der Bedrohungslage und des Gefährdungspotenzials durch dieses Phänomen, die Materie einmal grundlegend aufzuschließen und darzulegen.
In Kooperation mit dem Nationalen Cyber-Abwehrzentrum (NCAZ) wurde der Projektteil zur Untersuchung des Hellfelds von Januar 2013 bis Januar 2014 durchgeführt.

2.2 Projektziele

Das Projekt möchte eine empirisch fundierte kriminalistisch-kriminologische Erkenntnisbasis zum Phänomen des Hacktivismus erschaffen. Zu einer solchen phänomenologischen Basis gehört auch die Grundlegung einer klaren begrifflichen Abgrenzung des Phänomens zu verwandten und ähnlichen phänomenologischen Strömungen.
Die Vorstellung von einer empirisch fundierten Phänomenologie gliedert sich in drei Bausteine, wovon jeder spezielle Fragestellungen beinhaltet und einen entsprechenden Erkenntnisgewinn generiert:

1. Basis-Phänomenologie: Hierzu zählen Daten zur Vorgehensweise und zu Verschleierungstechniken sowie zur Infrastruktur bzgl. der Kommunikation, Logistik und Timing.
2. Szene-Trend: Hier werden Informationen zu Entwicklungen und Trendwechseln, aktuelle Szenedynamiken, Schäden aber auch zu begrifflichen Abgrenzungen zusammengeführt.
3. Täter-Typologien: Hierunter fallen Aussagen zum Einzeltäter aber auch zu Tätergruppierungen wie z. B. Motive und Ideologien sowie soziodemographische und -ökonomische Merkmale.

Die Menge an (wissenschaftlicher) Literatur zum Phänomen Hacktivismus im deutschsprachigen und angelsächsischen Raum ist bislang überschaubar. Wenn das Phänomen behandelt wird, dann häufig peripher im Rahmen der Auseinandersetzung mit anderen

Phänomenen aus dem Bereich „Cyber“, wie z. B. Cybercrime-Delikte in Form von Phishing, Online-Betrug und Hacking, Cyberterrorismus und Cyberwar. (Publizierte) Wissenschaftliche Untersuchungen von Hacktivismus und Hacktivisten sind rar, es liegen wenig Ergebnisse quantitativer Untersuchungen wie z. B. Nutzerbefragungen sowie qualitativer Untersuchungen wie z. B. Auswertungen von Pressemitteilungen vor.

Damit stellt die vorliegende Studie mit der Umsetzung der angestrebten Ziele eine Erweiterung der bisherigen Wissens- und Erkenntnisbasis über das Phänomen Hacktivismus – und damit auch des Untersuchungsfeldes Cybercrime insgesamt – dar.

3 Methoden

3.1 Angemessenheit der Methode am Forschungsgegenstand

Der Forschungsgegenstand, der theoretische Zugriff auf diesen und die damit verbundenen Fragestellungen bestimmen die Wahl der Methode. Gleichzeitig wird der Zugang zum Untersuchungsgegenstand durch verschiedene Methoden unterschiedlich stark eingegrenzt bzw. ermöglicht, d. h. dass die gewählte Methode mitbestimmt, was genau untersucht werden kann. Hier gilt es einen Ausgleich in dem Sinne zu erlangen, dass die gewählte Methode den bestmöglichen und umfangreichsten Zugang zum Forschungsgegenstand sowie eine entsprechende Gültigkeit der Ergebnisse gewährt. Für letztgenannten Punkt ist es notwendig, vorher abzuklären, welche Gültigkeit der Ergebnisse angestrebt wird und welche Aussagen mit den Ergebnissen getroffen werden sollen.[2]

Daneben spielt bei der Wahl der Methode auch die Umsetzbarkeit im Forschungsfeld eine Rolle, wozu u. a. auch die vorhandenen zeitlichen, finanziellen und personellen Ressourcen gehören.

Die drei Projektziel-Bausteine verfolgen mit dem Erzeugen einer empirisch fundierten Phänomenologie ein deskriptives Forschungsziel, für welches sich ein deskriptiver Zugang zum Untersuchungsgegenstand anbietet.

Zur Umsetzung der drei Bausteine (Kapitel 2.2) wurde zuerst mittels Analyse von Fachliteratur (Sekundäranalyse bzw. Metaanalyse) eine Erhebung des (aktuellen) Forschungsstands zum Phänomen Hacktivismus durchgeführt. Diese diente zum einen der Verortung des Forschungsthemas in dem vorhandenen Wissensstand und zum anderen der Gewinnung von Erkenntnissen zum Phänomen vor dem Hintergrund der Projektziel-Bausteine.[3] Zudem liefern die Ergebnisse ergänzende Hinweise für die Konstruktion der Fallanalyse bzw. des zugehörigen Erhebungsinstruments (Kapitel 3.3.1).

In der Orientierungsphase der Sekundäranalyse wird das Untersuchungsfeld anhand der Sichtung und Auswertung vorhandener Literatur sowie quantitativer und qualitativer Studienergebnisse zum Phänomen breitgefächert aufgeschlossen[4]. In der anschließenden

[2] Raab-Steiner,E./Benesch,M. (2008). *Der Fragebogen. Von der Forschungsidee zur SPSS-Auswertung*. Facultas wuv. S. 37

[3] Bortz, J./Döring, N. (2006). *Forschungsmethoden und Evaluation für Human- und Sozialwissenschaftler*. Springer Medizin Verlag. S. 47 ff.

[4] Explizite wissenschaftliche Abhandlungen zum Hacktivismus sind selten. Daher wurden auch Abhandlungen ausgewertet, die sich im Schwerpunkt einem anderem Cyberphänomen widmen, Hacktivismus jedoch peripher bzw. im Zusammenhang thematisieren.

Vertiefungsphase werden die gefundenen themenrelevanten Erkenntnisse und Ergebnisse erhoben, verglichen und in einem Dokumentationsbericht dargestellt und zusammengefasst.

Um über die sekundäre Analyse von bereits vorhandenen Erkenntnissen hinaus Aussagen, und hier vor allem empirisch fundierte Aussagen, über Hacktivisten und Hacktivismus treffen zu können, steht die Analyse hacktivistischer Taten und Ereignisse im Methodenfokus. Hierfür bietet es sich an, Fälle zu analysieren, die definitiv als Hacktivismus deklariert wurden und zu denen Zugang besteht. Diesen Zugang bieten Fall- und Ermittlungsakten der Polizeien und Staatsanwaltschaften, die Taten als hacktivistisch ausgerichtet ausweisen und darüber hinaus diverse Informationen enthalten, die die Projektziele (festgehalten in den drei Bausteinen) bedienen können.
Diese Art der Fallanalyse generiert ausschließlich Aussagen zu hacktivistischen Aktivitäten und Tätern, die es ins Hellfeld „geschafft“ haben und genügt damit der Ausrichtung dieses Projektteils (Hellfeld). Erkenntnisse über hacktivistische Taten im Dunkelfeld lassen sich auf diese Weise nicht erlangen. Ob sich die Erkenntnisse über das Hellfeld mit dem Dunkelfeld decken, ließe sich vereinzelt mit dem Vergleich von Ergebnissen aus der Sekundäranalyse feststellen, da hier auch Aussagen aus (qualitativen) Studien des Dunkelfeldes vorliegen, die jedoch nicht zwangsläufig hoch repräsentativ und generalisierbar sein müssen. Hier gilt es in der Vergleichbarkeit und Zusammenfassung der Ergebnisse aus Fall- und Sekundäranalyse Vorsicht walten zu lassen, es ist jedoch für diesen Projektteil nicht beabsichtigt einen derartigen Abgleich durchzuführen.[5]

Beide Methoden gewähren Anonymität und genügen damit den ethischen und datenschutzrechtlichen Ansprüchen an ein Forschungsprojekt.[6]

3.2 Sekundäranalyse

3.2.1 Materialerhebung

Mit dem Ziel den aktuellen Forschungsstand möglichst lückenlos zu erfassen, wurde die Analyse vorhandener Forschungsliteratur zum Phänomen Hacktivismus in einem sechsmonatigen Zeitraum von März 2013 bis August 2013 durchgeführt.

[5] Die Erforschung des Dunkelfelds war nicht Ziel des ersten Projektteils. Im zweiten Projektteil, der im Februar 2014 startete, wird das Dunkelfeld für den Bereich Hacktivismus untersucht.
[6] Physische oder psychische Risiken sowie die Einhaltung des Rechts auf Privatsphäre spielten mit den gewählten Methoden in dem Projekt keine Rolle.

Für die Sekundäranalyse wurde folgende analytische Definition[7] zu Grunde gelegt:

> *Hacktivismus setzt sich aus den Konzepten des Hackings und des Aktivismus zusammen. Die Schnittstelle beider Konzepte erklärt hacktivistische Ausrichtungen. Es handelt sich demnach um ideologisch, sozial und/oder politisch motivierte Aktionen unter Nutzung von Hacking-/IuK-Tools. Computer und Netzwerke sind Tatmittel und Angriffsziele zugleich. Sie werden als Protestmittel zur Verdeutlichung politischer und/oder gesellschaftlicher Ideologien eingesetzt. Die Taten sind nicht profitorientiert, es geht nicht um das missbräuchliche Erlangen von materiellem und/oder finanziellem Gewinn.*

Die Untersuchung fokussierte primär auf wissenschaftlich fundierten Arbeiten, die hauptsächlich in Universitäts- und Institutsbibliotheken sowie durch Recherche in entsprechenden Internetportalen, unterschiedlichen Katalogen und Suchmaschinen gefunden wurden.[8] Neben Studien und Fachliteratur wurden auch Medienberichte sowie Berichte und Studien der IT-Branche gesichtet.

In der Orientierungsphase wurde ein erster Überblick über die vorhandene Literatur zum Phänomen Hacktivismus gewonnen. Nach einer Ausdifferenzierung der Begrifflichkeiten Hacktivisten, Hacker, Internetaktivisten, Cyberterroristen, Cyberkriminelle und Cyberkriegsführung, dienten u. a. folgende Schlagwörter als Suchkriterium: Hacktivisten, Hacktivismus, politische Aktivisten, Internetkriminalität, Hacktivsm, Cybercrime etc.

Ausgehend von diesem Literaturfundus wurde die Bibliographie in der Vertiefungsphase gezielt über Quellenverweise beständig erweitert. In einer gezielten Detailsuche wurden Studien und Artikel in die Arbeit aufgenommen, die ihren Schwerpunkt auf andere Phänomene aus dem Cyber-Bereich gesetzt haben, die jedoch peripher Erkenntnisse zu Hacktivismus lieferten. Hierbei dienten u. a. Schlagwörter wie Hacker, Hacking, Netzaktivismus, Cyberterrorismus oder Internetkriminalität als Suchkriterium.

---

[7] „*Eine analytische Definition klärt einen Begriff durch die Analyse seiner Semantik und seiner Gebrauchsweise (Bedeutungsanalyse). Analytische Definitionen müssen empirisch überprüfbar sein*." (Bortz/Döring 2006, S. 62)

[8] Es wurde keine Selektion eines bestimmten Zeitraums, in welchem das recherchierte Material veröffentlicht wurde, vorgenommen.

3.2.2 Auswertung

Die erhobene Literatur wurde anhand der Ziel-Bausteine *Basis-Phänomenologie* (Erkenntnisse zur Vorgehensweise, zu Verschleierungstechniken sowie zur Infrastruktur bzgl. der Kommunikation, Logistik und Timing), *Szene-Trend* (Informationen zu Entwicklungen und Trendwechseln, aktuelle Szenedynamiken, Schäden, begriffliche Abgrenzungen) und *Täter-Typologien* (Aussagen zum Einzeltäter, zu Tätergruppierungen wie z. B. Motive, Ideologien sowie soziodemographische und -ökonomische Merkmale) ausgewertet (s. Kapitel 4). Das Vorgehen und die Ergebnisse der Analyse wurden in einem abschließenden Bericht[9] festgehalten, der in den vorliegenden Gesamtbericht einfloss.

Insgesamt wurden 184 Quellen in Form von Büchern, Berichten, Studien und Artikeln ausgewertet. Die erhobene und ausgewertete Literatur umfasst in zeitlicher Hinsicht mit Ausnahme zweier Veröffentlichungen aus den Jahren 1994 und 1997[10] die Erscheinungsjahre von 2000 bis 2013 (s. Abbildung 2).

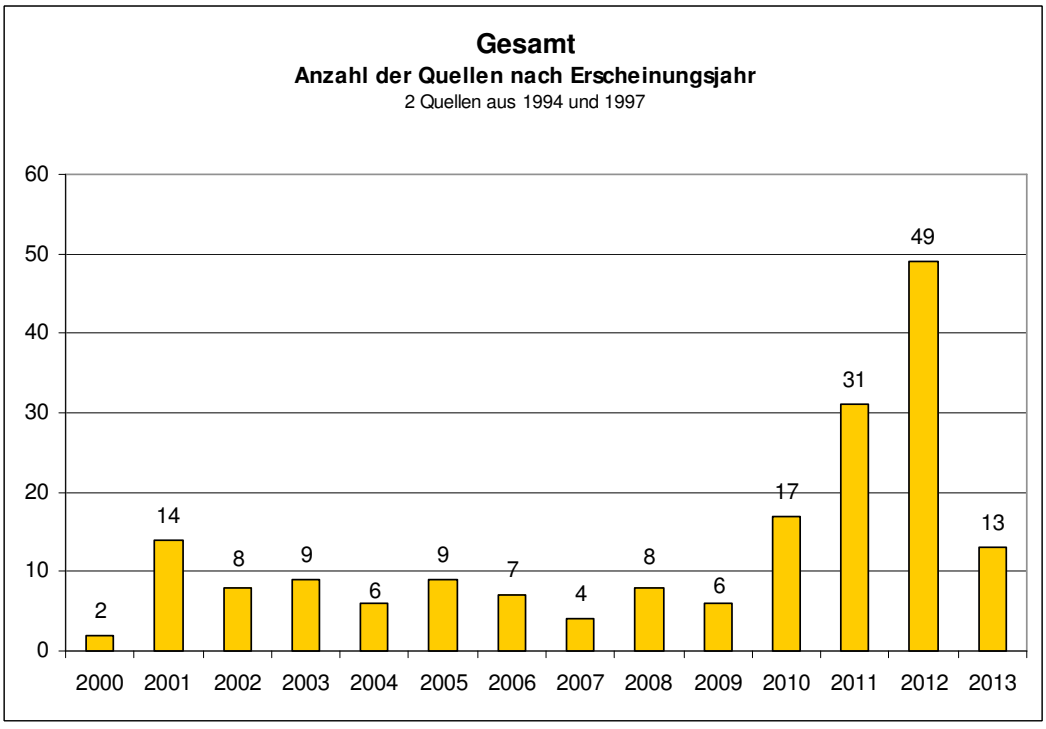


Abbildung 2: In der Sekundäranalyse ausgewertete Quellen.

[9] Der Bericht zur Sekundäranalyse liegt intern vor.
[10] Hierbei handelt es sich um The Knightmare/Branwyn, G. (1994). *Secrets of a Super Hacker*. Loompanics Unlimited und um Bühl, A. (1997). *Die virtuelle Gesellschaft*. Ökonomie, Kultur und Politik im Zeichen des Cyberspace. Westdeutscher Verlag.

Das ausgewertete Material wurde elf verschiedenen Kategorien zugeordnet, die den Ursprungskontext wiedergeben, in welchem Hacktivismus abgehandelt wurde bzw. die Schnittstellen zu anderen Phänomenen markieren: Hacktivismus, Hacker, Internetaktivisten, Cyberterrorismus, Cyberkriminalität, Techniken/Malware/Botnetze, Cyberkriegsführung, Insider, Kultur, Reviews, Zeitungsartikel (s. Anlage 1).

Von den 184 ausgewerteten Quellen befassten sich 54 schwerpunktmäßig mit Hacktivismus. 19 Quellen beschäftigten sich primär mit Hackern und elf mit Internetaktivisten. Aus dem Bereich Terrorismus und Cyberterrorismus wurden 22 Quellen ausgewertet, die sich peripher mit Hacktivismus beschäftigten, sowie 12 Quellen aus dem Bereich der sonstigen Cybercrime und 35 der ausgewerteten Quellen ließen sich der Kategorie Techniken/Malware/Botnetze zuordnen. Für die genannten Kategorien gilt, dass hier die meisten der Quellen aus dem Jahr 2012 stammen.
Des Weiteren wurden 13 Zeitungsartikel ausgewertet sowie Quellen aus dem Bereich Cyberkriegsführung (6), Insider (5), Kultur (4) und Reviews (4).

3.3 Fallanalyse

3.3.1 Datenerhebung

Da mit dem Projekt Neuland betreten wurde, wurde die Fallanalyse als empirisch-quantitative Exploration und Deskription angelegt. Ziel war es mittels umfangreicher Aufbereitung und Auswertung quantitativer Daten etwaige Zusammenhänge zwischen verschiedenen Variablen zu entdecken und ggf. Hypothesen aus den Erkenntnissen der Untersuchung abzuleiten.

Im ersten Projektteil sollte das Hellfeld untersucht und aus den gefundenen Daten entsprechende Aussagen zu den Ziel-Bausteinen generiert werden. Hacktivismus im Hellfeld bedeutet, dass es sich hierbei um alle hacktivistische Aktivitäten handelt, die offiziell, d. h. der Polizei, bekannt und registriert[11] sind. Da die Vermutung bestand, dass die Zahl polizeibekannter Fälle von Hacktivismus unter ca. 300 liegen wird[12], entschieden sich die

[11] Offiziell bekannte Straftaten werden in der Polizeilichen Kriminalstatistik (PKS) erfasst. Für hacktivistische Taten gibt es keinen einheitlichen Summenschlüssel in der PKS (so wie es auch für weitere Delikte von Cybercrime keine Schlüssel gibt). Diese Taten werden je nach angewendetem Straftatbestand unterschiedlichen Schlüsseln zugeordnet.
[12] Diese Vermutung wurde von einer Interpretation der PKSen und der Strafverfolgungsstatistiken der letzten Jahre vor dem Hintergrund infrage kommender angewandter Straftatbestände sowie einer überblicksartigen Sichtung von Nachrichten und Schlagzeilen hacktivistischer Ereignisse der letzten zehn Jahre in Deutschland gestützt.

Projektbeteiligten gegen eine Stichprobenerhebung und für eine Vollerhebung aller hacktivistischer Fälle der letzten Jahre in Deutschland.

Im März 2013 wurden die Landeskriminalämter sowie die Landesjustizverwaltungen aller Bundesländer in Deutschland angeschrieben, mit der Bitte um Weiterleitung der Anfrage an entsprechende Dienststellen bzw. Staatsanwaltschaften und mit der Bitte um Zulieferung von Ermittlungs- und Fallakten mit hacktivistischem Tathintergrund.
Vor der Erhebung wurde eine analytische Definition von Hacktivismus festgelegt (Kapitel 3.2.1), die den angeschriebenen Instituten als Leitfaden bei der Selektion relevanter Fälle diente und wie folgt lautet[13]:

„[…]

in den letzten Jahren sind vermehrt spektakuläre Aktionen hacktivistischer Art in den Fokus der Öffentlichkeit und der Strafverfolgungsbehörden gerückt. Hierbei handelt es sich um Online-Hacker-Aktivitäten in Kombination mit politischem und sozialem Aktivismus. IuK-Technologien wie Computer und Netzwerke sind Tatmittel und Angriffsziele zugleich. Daneben werden sie als Protestmittel zur Verdeutlichung politischer und/oder gesellschaftlicher Ideologien genutzt.

Relevante Straftatbestände bei hacktivistischen Aktivitäten können vor allem (jedoch nicht ausschließlich) Kombinationen aus folgenden Strafnormen des Strafgesetzbuches sein:

§§ 202 a, b, c – § 263 a – § 269 – §§ 303 a, b StGB

Eine Analyse weiterer relevanter Straftatbestände und entsprechender Lagebilder hat bereits die Erkenntnis erbracht, dass Straftaten von Hacktivisten häufig auch als Staatsschutzdelikte (PMK) mit Tatmittel Internet erfasst werden, so dass die Einbeziehung der Staatsschutz-Dienststellen ihres Zuständigkeitsbereichs angeregt wird.

Abbildung 3: Analytische Definition im Anschreiben.

[.]“

Der Erfolg der angestrebten Vollerhebung war abhängig von den Zulieferungen der angeschriebenen Stellen: Hier besteht die Vermutung, dass es im Ergebnis nicht zu einer korrekten (i. e. S.) Vollerhebung polizeibekannter hacktivistischer Fälle kam, da die Wahrscheinlichkeit besteht, dass zum einen nicht alle hacktivistischen Fälle von den Dienststellen als solche identifiziert werden konnten und dass zum anderen einige (nicht alle) Dienststellen, die Fehlanzeige meldeten, dies aufgrund fehlender zeitlicher und/oder personeller Ressourcen für die Identifizierung von Akten mit hacktivistischem Hintergrund taten.[14]

[13] Auszug aus den Anschreiben an die Landespolizeidienststellen und Staatsanwaltschaften aller Bundesländer der Bundesrepublik Deutschland.
[14] Lässt man diese Vermutungen außen vor, ist das Ergebnis eine Vollerhebung (andernfalls handelte es sich um eine nicht kontrolliert erhobene Stichprobe).

Im Falle eines spezifischen Verfahrens konnten die entsprechenden Fälle bei den betroffenen Staatsanwaltschaften vollständig gezogen werden.

Mit den ersten Zulieferungen begann die Sichtung der Akten und eventuelles Aussortieren nicht relevanter Fälle, d. h. Fälle ohne hacktivistischen Bezug. Insgesamt lagen 183 Fallakten zur Auswertung vor. Davon kommen 106 Akten auf ein Verfahren (s. o.), daneben liegen fünf weitere Akten der Staatsanwaltschaften zu anderen Verfahren vor. Die Polizeien der Bundesländer lieferten insgesamt 72 Fallakten zu. Nordrhein-Westfalen, Baden-Württemberg, Niedersachsen, Bayern und Hessen lieferten – sowohl insgesamt als auch nach Zulieferungen der Staatsanwaltschaften differenziert – den Großteil der Akten zu:

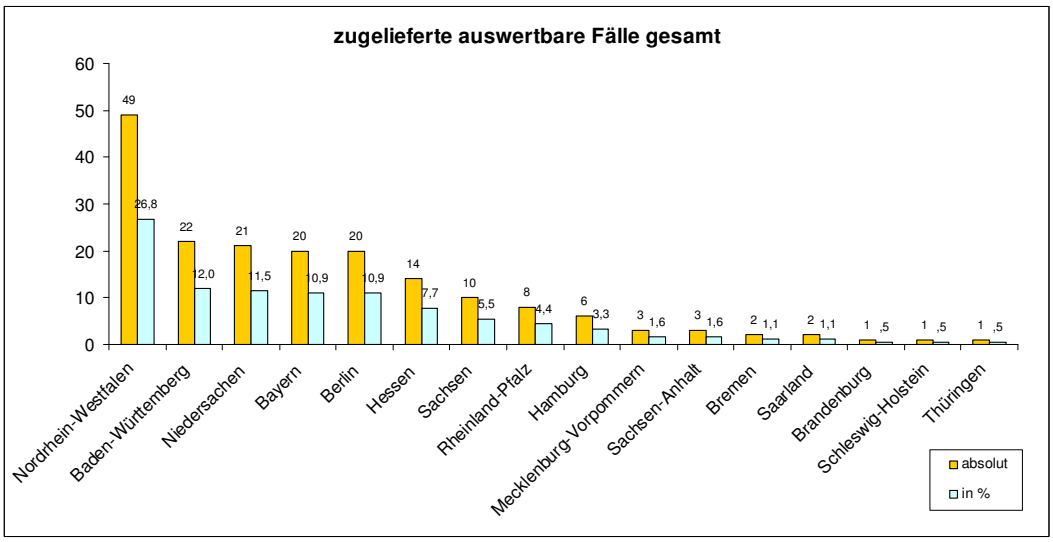


Abbildung 4: Zulieferungen aus den Bundesländern.

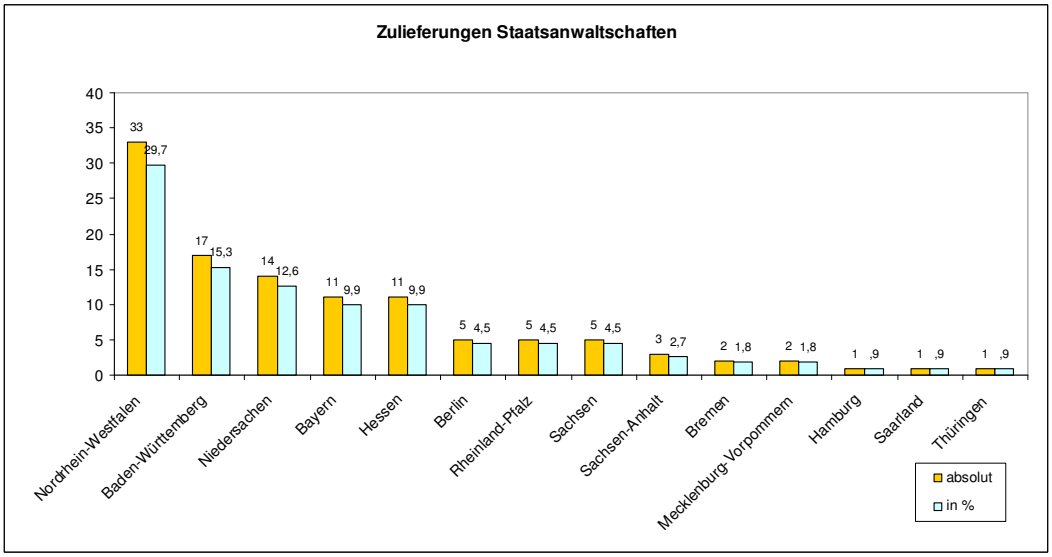


Abbildung 5: Zulieferungen der Staatsanwaltschaften.

Der Großteil polizeilicher Akten wurde von Nordrhein-Westfalen, Berlin und Bayern zugeliefert:

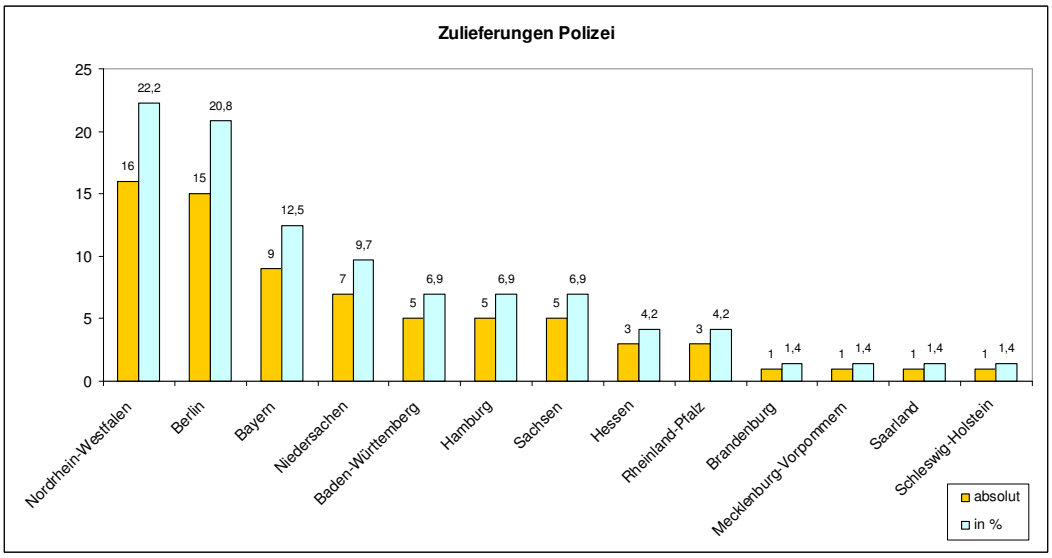


Abbildung 6: Zulieferungen der Polizeien.

3.3.2 Auswertung

Im Vorfeld der Auswertung wurde ein Erhebungsinstrument entwickelt, der sog. Erhebungsbogen. Dieser enthielt einem Fragebogen ähnlich Items, anhand derer die Fallakten überprüft und ausgewertet werden. Die Items sind die operationalisierten (d. h. messbar gemachten) Informationen, die in den Ziel-Bausteinen (*Basis-Phänomenologie, Szene-Trend, Täter-Typologien*) beschrieben werden und die erforderlich für die Generierung von Aussagen zum Phänomen sind.

Mit der ersten Sichtung der Akten konnte anhand der vorgefundenen Informationsqualität und -quantität der Akten die Abdeckung der vorhandenen Informationen durch die Items des Erhebungsbogens überprüft werden. Der Erhebungsbogen wurde dann um einige operationalisierte Items ergänzt und modifiziert (s. Anlage 2).

1	Bundesland			1	1=BW; 2=BY; 3=BR; 4=BB; 5=HB; 6=HH; 7=HE; 8=MV; 9=NI; 10=NW; 11=RP; 12=SL; 13=SN; 14=SA; 15=SH; 16=TH
2	Verfahren	Status des Verfahrens zum Zeitpunkt der Abfrage		2	1= laufendes Verf.; 2= abgeschlossenes Verf.; 99=k.A.
3	Tatzeit1	Zeitpunkt des Bekanntwerdens		3	Datum und/oder Uhrzeit
4	Tatzeit2	Zeitpunkt erneuten Bekanntwerdens		4	"
5	Ort	Ort des Geschädigten/ Tateintritts		5	Bundesland; Stadt o. ä.
6	Straftat1	verletzte Rechtsnorm		6	1=202a StGB; 2=303a StGB; 3=303b StGB; 4=263aStGB; 5=269 StGB; 6=270 StGB; 7=202b StGB; 8=202c StGB
7	Straftat2			7	"
8	Straftat3			8	"
9	Straftat4			9	" [7=Dienstleistungsunternehmen; 8=Behörden; 9=Medien/Presse; 91=Freiberufler
10	Geschädigter			10	1=Privatperson; 2=Schule; 3=Online-Versandhaus; 4=Verein/Kirche; 5=Partei; 6=Produktionsbetrieb;
11	Wirkung	Zielrichtung/Wirkung der Tat		11	1=Inhalt/Darstellung Webseite; 2=Betrieb einer Dienstleistung Webseite; 3=Erreichbarkeit Server;
12	Schadenshöhe	finanzieller Schaden		12	in Euro 4=Integrität Datenbestand

Abbildung 7: Auszug aus dem Erhebungsbogen.

Die Erhebungs- und Auswertephase konnte im November 2013 abgeschlossen werden. An diese Phase schloss sich eine explorative quantitative Datenanalyse in Form einfacher Deskriptivanalysen[15] mittels der Statistiksoftware SPSS 21 an (Auszug siehe Anlage 3). Ende Dezember 2013 wurde die Datenanalyse abgeschlossen und das anschließende Expertenarbeitstreffen vorbereitet.

3.4 Expertenarbeitstreffen

3.4.1 Inhalte und Ablauf

Am 14.01.2014 fand das Expertentreffen zum Projektteil Hellfeld statt. Ziel des Treffens war die Diskussion und Bewertung der Ergebnisse aus Sekundär- und Fallanalyse vor dem Hintergrund verschiedener Perspektiven und Erfahrungsschätze.

Darüber hinaus sollten aus den Ergebnissen der Analysen Implikationen erörtert und Handlungsempfehlungen abgeleitet werden.

An dem Treffen nahmen insgesamt 24 Experten teil, die von unterschiedlichen Institutionen aus den Bereichen Cybercrime (Polizei und Staatsanwaltschaft), polizeilicher Staatsschutz und kriminalistisch-kriminologischer Forschung kamen.

[15] Einfache deskriptive Analysen sind Häufigkeitsverteilungen, Maße der zentralen Tendenz und Dispersion, Kreuztabellen und Korrelationsmatrizen und dienen der Vergleichbarkeit von Daten und der Erkennung von Merkmalszusammenhängen (Bortz/Döring 2006, S. 371).

Um eine umfassende Betrachtung unterschiedlicher Aspekte des Phänomens sowie der Analyseergebnisse sicherzustellen, wurde als Methode für das Treffen die Durchführung von Arbeitsgruppen[16] gewählt. Um bestmögliche Arbeitsergebnisse zu erzielen, wurden die Problem- und Fragestellungen für die Arbeitsgruppen sowohl an den Ergebnissen der Analysen und phänomenspezifischen Theorien ausgerichtet als auch an den unterschiedlichen Professionen der Experten orientiert.

Interessant war, wie die Ergebnisse und Aussagen der Sekundär- und Fallanalyse zum Phänomen von den Experten, die in der Praxis unterschiedliche Berührungspunkte mit dem Phänomen haben, aus deren entsprechenden Perspektiven bewertet werden würden.
Von Relevanz für die Erarbeitung von Handlungsempfehlungen ist auch die Betrachtung des Dunkelfelds, d. h. welche Vermutungen über die Größe eines Dunkelfelds hacktivistischer Aktivitäten es gibt und wie diese begründet werden bzw. sich begründen lassen.
Aufschlussreich (insbesondere vor dem Hintergrund weiterführender Forschung im zweiten Projektteil) war auch die Frage nach Erschließungsmöglichkeiten des Dunkelfelds. Des Weiteren sollte der kriminologische Aspekt der „Hemmschwelle“ eine Rolle spielen: Erleichtert das digitale Umfeld Personen, die bislang an analogen Formen von Aktivismus nicht teilgenommen haben, die Partizipation an (h)a(c)ktivistischen Aktionen? Zu diskutieren waren hier z. B. Cybercrime-typische kriminogene Faktoren, d. h. Faktoren, die die Hemmschwelle zur (digitalen) Tatbegehung herabsetzen. Hierzu gehörte auch die Frage nach dem Unrechts- und Straftatenbewusstsein der Partizipierenden. Der Aufarbeitung solcher und weiterer Aspekte zum Punkt „Hemmschwelle“ sollten Überlegungen zu möglichen repressiven und präventiven Implikationen folgen.

Das Problem des definitorischen, rechtlichen und statistischen „Erfassens“ hacktivistischer Taten kam auch bei der Entwicklung von Handlungsempfehlungen zum Tragen. Ist es notwendig, das Phänomen Hacktivismus statistisch dezidierter zu erfassen; müssen neue Straftatbestände und strafprozessuale Anordnungen geschaffen oder bestehende lediglich angepasst werden; welche Rolle spielt eine klare definitorische Abgrenzung von Hacktivismus zu anderen (Cybercrime-)Phänomenen? All diese Fragen bedurften einer weiteren Erörterung, beinhalteten sie bereits Anhaltspunkte für weitere Implikationen.

[16] i. S. der Gruppenbefragungstechniken Gruppendiskussion und Moderationsmethode (vgl. Bortz/Döring 2006, S. 319 f.)

Zudem war es ein Anliegen, im Projekt die Frage nach dem Ausprägungsgrad des Gefährdungs- und Schadenspotenzials von Hacktivismus zu klären. Vor allem in der Bewertung der Relevanz und der Gewichtung verschiedener Optionen von Handlungsempfehlungen war die Klärung der Frage wichtig, welches Potenzial (sowohl im negativen als auch im positiven Sinne) das Phänomen hat und haben kann.
Ein letzter Schritt bei der Erarbeitung von Handlungsempfehlungen war das Konstruieren und Betrachten möglicher (zukünftiger) Szenarien, anhand derer sich aufzeigen lassen, wo Risiken aber auch Verbesserungspotentiale liegen, an die Handlungsempfehlungen anknüpfen können.

3.4.2 Phänomenbezug der Teilnehmer

Zu Beginn wurden die Teilnehmer aufgefordert, sich mit dem Anteil des Phänomens am dienstlichen Alltag sowie mit dem persönlichen oder dienstlichen Interesse in einem Koordinatensystem zu verorten. Es lässt sich festhalten, dass die Mehrzahl der Teilnehmer bislang wenige Berührungspunkte mit dem Phänomen Hacktivismus im dienstlichen Alltag hatte, lediglich vier Teilnehmer aus dem Staatsschutz und ein Teilnehmer aus der Strafverfolgung wiesen hier einen mittleren bis höheren Anteil aus. Das persönliche bzw. dienstliche Interesse an dem Phänomen war breit gestreut, die Mehrheit der Teilnehmer hat sich bei mittlerem bis hohem Interesse an dem Phänomen verortet.[17]

3.4.3 Arbeitsgruppen

Mit dem Arbeitstreffen konnte auf einer breiten Basis an Expertenwissen und Perspektiven ein reger und vielfältiger Austausch stattfinden. Es wurden ertragreiche und fruchtbare Diskussionen geführt und letztlich perspektivisch verschiedene Argumente und Ideen hervorgebracht.

Aufgrund der zeitlich kompakten Gestaltung und Ausrichtung des Arbeitstreffens und des Strebens nach einer umfassenden Betrachtung des Phänomens mit seinen unterschiedlichen Aspekten wurde bewusst der intensive Einsatz von Arbeits- und Diskussionsgruppen längeren Vorträgen und Plenumsdiskussionen vorgezogen. Mit dem Einsatz kleiner und möglichst

[17] Daneben äußerten einige Teilnehmer Wünsche und Erwartungen an die Veranstaltung. Diese waren u. a.:
- In einen persönlichen und regen Austausch miteinander zu kommen.
- Kontakte knüpfen und das eigene Netzwerk erweitern.
- Interessante Diskussionen (auch als Input für Folgeveranstaltungen) zu führen.
- Erkenntnisse aus der Forschung und eine begriffliche Abgrenzung des Phänomens erfahren.
- Möglichkeiten einer optimierten Zusammenarbeit aufzeigen und Input für Vernehmungen mitnehmen.
- Diskussionen über die Zuständigkeiten, Strafbarkeit und Tätergruppen in dem Phänomenbereich führen.

homogener Gruppen wurden gruppendynamische Bedingungen geschaffen, die den Gruppenprozess günstig beeinflussten und die es jedem Teilnehmer ermöglichten aktiv mitzuarbeiten.[18] Zudem regen Ideen anderer Teilnehmer eigene Gedanken an, welche in kleineren Gruppen eher zur Geltung kommen können, als in großen Plenen, in denen sich der Einzelne mit seinen Ideen eher verliert bzw. zurückzieht.[19] Daher sind die Qualität und der Ertrag von Diskussionen in kleineren Gruppen oftmals höher zu bewerten als in großen Plenen.
Zudem bietet der Einsatz von Diskussions- und Arbeitsgruppen in einem zeitlich kompakten Treffen den Vorteil, dass mehrere Fragestellungen und Aspekte in verschiedenen Gruppen parallel diskutiert und bearbeitet werden können (sog. Fokusgruppen)[20], und dennoch ein ganzheitlicher Output für alle Teilnehmer generiert wird.

Um kleine und möglichst homogene Fokusgruppen[21] zu erhalten, wurden die Teilnehmer im Vorfeld entsprechend ihrer Profession bzw. ihrem Beschäftigungsbereich eingeordnet:
Zehn Teilnehmer kamen aus dem Bereich der Strafverfolgung, sieben Teilnehmer aus dem Bereich des Staatsschutzes[22] und weitere sieben Teilnehmer kamen aus dem kriminalistisch-kriminologischen Forschungsbereich.

Für die Fokusgruppen wurde die Moderationsmethode als besondere Form der Organisation von Gruppenprozessen eingesetzt. Die Moderationsmethode zielt darauf ab, alle Teilnehmer gleichberechtigt an den Arbeitsgruppen zu beteiligen. Daneben wurden alle Arbeitsschritte, Fragestellungen sowie zu diskutierende Aspekte geplant. Die Arbeitsgruppen und die einzelnen Arbeitsschritte wurden strukturiert und moderiert durchgeführt. Durch

[18] Dreher, M./Dreher, E. (1994). *Gruppendiskussion*. In: Huber, G./Mandl, H. (Hrsg.). *Verbale Daten. Eine Einführung in die Grundlagen der Erhebung und Auswertung*. Beltz Verlag. S. 141 ff.
[19] Lamnek, S. (1993). *Qualitative Sozialforschung. Band 2: Methoden und Techniken*. Psychologie Verlags Union. S. 166 ff.
[20] Dürrenberger, G./Behringer, J. (1999). *Die Fokusgruppe in Theorie und Anwendung*. Stuttgart: Akademie für Technikfolgenabschätzung in Baden-Württemberg
[21] Die Homogenität einer Fokusgruppe zeichnet sich hierbei durch die Zugehörigkeit aller bzw. der meisten Teilnehmer zu einem Professions- bzw. Beschäftigungsbereich aus.
[22] Ein Teil der Teilnehmer, die dem Bereich „Staatsschutz“ zugeordnet wurden, ließen sich auch dem Bereich der Strafverfolgung zuordnen (repressiver Staatsschutz). Um jedoch eine annähernd gleichmäßige Aufteilung der Teilnehmer zu den Arbeitsgruppen entsprechend ihrem Professionsgebiet zu ermöglichen, wurde diese Zuordnung gewählt.

Visualisierungen[23] wurden die Arbeitsergebnisse für alle Teilnehmer des Treffens veranschaulicht.[24]

Für die Fokusgruppen wurden insgesamt sieben Problem- und Fragestellungen strukturiert, die mittels Gruppendiskussion, Brainstorming, Befragung und Visualisierung von den Teilnehmern konstruktiv er- und bearbeitet wurden. Die Ergebnisse wurden jeweils auf farbigen Karten festgehalten und an Stellwänden oder vorbereiteten Plakaten befestigt. Bei den sieben Themen/Fragestellungen handelte es sich um die folgenden:

- Darstellung des eigenen dienstlichen Bezugs zum Phänomen Hacktivismus sowie des (persönlichen oder dienstlichen) Interesses am Phänomen. Vorstellung der eigenen Person und (optionale) Benennung von Erwartungen und Wünschen an das Arbeitstreffen. (1.)
- Nach der Vorstellung der Ergebnisse aus Sekundär- und Fallanalyse wurden die Ergebnisse vor dem Hintergrund eigener Erfahrung aus der Praxis bzw. eigener Vermutungen (sofern Praxiserfahrung nicht vorhanden war) mit dem/den jeweiligen Dienstpartner/n bewertet. (2.)
- Vier inhomogene Diskussionsgruppen[25] zu den vier Themen *Dunkelfeld, Hemmschwelle, Erfassen von Hacktivismus* und *Gefährdungspotenzial*. (3.-6.)
- Negatives Brainstorming[26] in vier homogenen Fokusgruppen. (7.)

Die Arbeitsgruppen erarbeiteten selbst strukturierte und konsensfähige Ergebnisse, entsprechend dem Ziel des Einsatzes der Moderationsmethode. Die Ideen der Teilnehmer zu den Aspekten und Fragestellungen wurden in den Arbeitsgruppen diskutiert, erörtert und auf Moderationskarten notiert, die ggf. innerhalb der Gruppe noch priorisiert und/oder selektiert wurden. Anschließend wurden diese auf die dafür vorgesehenen und der Fragestellung

[23] Visualisierungstechniken sind hierbei Plakate, Stellwände, Flipcharts, farbige Karten, Filzstifte und Klebepunkte.

[24] Vorteile der Moderationsmethode sind, dass die Teilnehmer mehr Spaß an der Sache haben, aktiver sind und mehr für sich und die eigene Arbeit mitnehmen. Insbesondere für Forschungszwecke lässt sich diese Methode gut im explorativen Bereich nutzen und war damit aus Projektsicht die am besten geeignete Methode für die beabsichtigte Zielrichtung des Expertentreffens.

[25] Hier war keine Gruppenhomogenität i. S. des Professions- und Beschäftigungsbereichs gewünscht, sondern die Teilnehmer durften sich nach eigener Interessenlage den Fokusgruppen zuordnen.

[26] Methode des Brainstormings, bei welcher die Fragestellung aus einer Worst-Case Ansicht heraus analysiert wird.

entsprechend vorbereiteten Plakate befestigt.[27] Die Ideen und Ergebnisse auf den Plakaten wurden im nächsten Schritt von allen Teilnehmern betrachtet und ggf. mit Anmerkungskärtchen versehen. Danach folgte die Besprechung der durch die Anmerkungskärtchen gekennzeichneten Ergebnisse und Ideen im gesamten Expertenkreis.

3.5 Selektionseffekte und Verzerrfaktoren

Das Ziel des Projektteils Hellfeld ist die Beschreibung von offiziell bekannten hacktivistischen Taten. Es wird nicht der Anspruch erhoben, generalisierbare Aussagen für die Grundgesamtheit hacktivistischer Aktivitäten zu erheben, d. h. ebenso Merkmale von Aktivitäten und Taten zu beschreiben, die sich im Dunkelfeld befinden. Das bedeutet, dass keine Rückschlüsse von den gewonnenen Ergebnissen auf das Dunkelfeld aufgrund bekannter Verzerreffekte durch Hellfeld-Dunkelfeld-Divergenzen gezogen werden können, dies jedoch auch in diesem Projektteil nicht vorgesehen ist.[28]
Die Repräsentativität der Ergebnisse und die Generalisierbarkeit der gewonnenen Aussagen muss hier in Bezug auf die Grundgesamtheit „offiziell bekannter Fälle von Hacktivismus" bewertet werden. Das bedeutet auch, dass die gewählte Grundgesamtheit hier über die Definition ausschließlich bekannter und registrierter Fälle von Hacktivismus sehr eingeschränkt ist.

Ausgehend von der Grundgesamtheit polizeibekannter Fälle, ist davon auszugehen, dass auch hier nicht alle Fälle zugeliefert wurden. Gründe hierfür können Verständnisprobleme mit der vorgegebenen Definition hacktivistischer Fälle gewesen sein, welche damit die Zuordnung entsprechender Taten zu dem Phänomen erschwert bzw. verhindert haben[29]. Daneben besteht die Möglichkeit, dass die Zulieferungsanfrage von den Landesjustizverwaltungen und/oder den Landeskriminalämtern nicht an alle (relevanten) Dienststellen gesteuert wurde bzw. vor Ort „unterging". Des Weiteren ist es wahrscheinlich, dass nicht alle Dienststellen die Ressourcen zur Auswahl und Sortierung entsprechender Fallakten gleichermaßen hatten und hier einige Fälle nicht zugeliefert werden konnten.

[27] Visualisierung der Aufgabenstellung mittels vorbereiteter Plakate und Stellwände sowie der Arbeitsgruppenergebnisse auf Moderationskarten und letztlich Visualisierung der gesamten Ergebnisse auf vorbereiteten Stellwänden.
[28] Bortz/Döring 2006, S. 480
[29] Es wurden jedoch lediglich 11 Fallakten zugeliefert, die nicht der vorgegebenen Definition entsprachen und lediglich zwei Anrufe erreichten die Projektverantwortlichen mit der Bitte um nähere Erläuterungen zur Definition.

Es ist jedoch nicht zu erwarten, dass aufgrund der vorgenannten Gründe a) die Zahl der nicht-zugelieferten Fälle übermäßig hoch ist und dass b) die nicht-zugelieferten Fälle spezielle Merkmale aufweisen, so dass bei einer (theoretischen) Einbeziehung dieser Fälle mit einer signifikanten Abänderung der Endergebnisse zu rechnen wäre.[30]

Mit der Methode der Sekundäranalyse hat man auch Ergebnisse aus Studien mit aufgenommen, die den Versuch unternahmen, das Dunkelfeld zu erhellen. Diese Ergebnisse sind denen der Fallanalyse sehr ähnlich (Kapitel 4). Eine genauere Untersuchung von Merkmalen hacktivisitischer Aktivitäten im Dunkelfeld folgt im zweiten Teil des Projekts.

[30] Bortz/Döring 2006, S. 397 f.

4 Ergebnisse

4.1 Begriffliche Abgrenzung

Eine Begriffsabgrenzung des Hacktivismus von anderen Erscheinungsformen von Cybercrime erscheint sowohl aus präventiver wie aus repressiver Sicht notwendig. In verschiedenen gesellschaftlichen Bereichen wie z. B. dem der privaten Internetnutzer, der Politik, der Wirtschaft aber auch der Sicherheitseinrichtungen herrscht noch immer kein einheitliches Verständnis der Zuordnung verschiedener Cybercrime-Delikte zu Phänomenbereichen. In der öffentlichen Kommunikation werden dabei Delikte oftmals fälschlicherweise einzelnen Phänomenen zugeordnet, so wie das Etikett „Hacktivismus“ häufig für Delikte Verwendung findet, die tatsächlich etwas anderes sind (wie z. B. Cyberterrorismus oder Netzaktivismus). Die Grenzen verschiedener Cybercrime-Phänomene verschwimmen jedoch nicht nur in der Kommunikation, auch in der Realität ist der Übergang von einem Phänomen zu einem anderen häufig fließend und nicht trennscharf.

In vielen Fällen ähneln sich die Vorgehensweisen und Tatmittel verschiedener Cybercrime-Phänomene, jedoch unterscheiden sich die Phänomene in Motivlage und Angriffsziel voneinander. Die Motive und Zielrichtungen der Deliktsbegehung sind entscheidend bei der Zuordnung von Taten zu Phänomenbereichen.

4.1.1 Hacktivismus vs. Hacking

Der Begriff Hacktivismus[31] beinhaltet die Konzepte Hacking und Aktivismus: Das Nutzen von Hacking- bzw. IuK-Tools für die Verdeutlichung und Durchsetzung bestimmter politischer wie sozialer Ziele (Ideologien) bildet die Schnittmenge beider Konzepte. Die Hacking-Tools werden hierbei u. a. für Protest- und/oder Propagandazwecke eingesetzt (Kapitel 4.2.7) und sind nicht profitorientiert, d. h. hacktivistische Taten zielen nicht darauf ab illegal materielle und finanzielle Gewinne zu erzielen (wie z. B. das Phishing).

Anders als finanziell motivierte Hacker veröffentlichen Hacktivisten aus ideologischen Gründen bspw. gestohlene Daten wie Zugangspasswörter, persönliche und vertrauliche Informationen, E-Mail-Adressen usw. im Internet.

[31] Der Ursprung des Begriffs wird mit der Mitte der 90er Jahre angegeben und mit der Bildung der Hackergruppe „Cult of the Dead Cow“ in Verbindung gebracht (Jordan, T./Taylor, P. (2004). *Hacktivism and Cyberwars. Rebels with a cause?*. Routledge. London)

Samuel definiert das Phänomen Hacktivismus als die „*Hochzeit von politischem Aktivismus und Computerhacking [...] als den gewaltfreien Gebrauch von illegalen oder legalen digitalen Werkzeugen um politische Ziele zu verfolgen.*"[32]
Als Hacker wurden anfänglich solche Personen bezeichnet, die besondere Fertigkeiten im Umgang mit Computern haben, ohne dass eine kriminelle Konnotation[33] bestand. Allgemein werden Hacker als Programmierexperten gesehen, die Spaß an der intellektuellen Herausforderung des Entwickelns und Modifizierens von Computerprogrammen und -systemen haben. Schon 1984 prägte der Journalist Steven Levy den Begriff der ‚Hackerethik', die folgende Grundwerte enthält:

> „*1. Zugang zu Computern – [...] – sollte unbegrenzt und umfassend sein. Mitmachen heißt die Devise.*
> *2. Alle Informationen sollten frei sein.*
> *3. Misstraue Autorität – fördere Dezentralisierung.*
> *4. Hacker sollten anhand ihres Hackens beurteilt werden, nicht nach unsinnigen Kriterien wie akademischen Rängen, Alter, Rasse oder Stellung.*
> *5. Du kannst mit einem Computer Kunst und Schönheit erzeugen.*
> *6. Computer können Dein Leben verbessern.*"[34]

Hampson unterscheidet Hacktivisten von Hackern auf Grundlage der Motive, die sie leiten.[35] Während Hacker von Eigeninteressen geleitet werden, verfolgen Hacktivisten oft soziale oder politische Ziele.

Gemein ist allen Definitionen, dass es sich bei Hacktivisten um „gewaltfreie" Aktivisten handelt, die sich der technischen Möglichkeiten von Internet und Computern auf vielfältige Art und Weise bedienen, um ideologisch motivierte Ziele zu verfolgen.

[32] Samuel, A.W. (2004). *Hacktivism and the Future of Political Participation*. Im Internet: http://www.alexandrasamuel.com/dissertation/pdfs/Samuel-Hacktivism-entire.pdf, S. 2
[33] Wie sie heutzutage insbesondere in der medialen Berichterstattung zu finden ist.
[34] Gröhndahl, B. (2001). *Scriptkiddies Are Not Alright*. In A. Medosch, J. Röttgers (Hrsg.): Netzpiraten. Die Kultur des elektronischen Verbrechens. Verlag Heinz Heise. Hannover, S. 144
[35] Hampson. N.C.N. (2012). *Hacktivism: A New Breed of Protest in an Network World*. In: B.C. International & Comparative Law Review pp. 511-542. http://lawdigitalcommon.s.bc.iclr/vol35/iss2/6

4.1.2 Cyberterrorismus

Aktionen von Hacktivisten oder andere Formen des Hackens werden oft als Cyberterrorismus missverstanden. Terroristen nutzen das Internet zur Ausführung von Angriffen, als Kommunikationsplattform (Propaganda) und zu Radikalisierungszwecken. Die wichtigste Abgrenzung zu Hacktivismus liegt im Ziel des Terrorismus begründet, nämlich Gewalt auszuüben, um einzuschüchtern und Schrecken und Leid zu verbreiten.[36] So fällt eine Attacke, die Services unterbricht, aber nicht mehr als finanzielle Kosten verursacht, nicht darunter.

Die Bedrohung kritischer Infrastrukturen durch digitale Angriffe wird derzeit noch kontrovers diskutiert (s. u.). Die herrschende Meinung ordnet solche Angriffe dem Cyberterrorismus zu; die Bedrohungslage wird derzeit als grundsätzlich vorhanden aber noch nicht aktuell brisant eingeschätzt.

Brickey (2012) definiert Cyberterrorismus als „*den Gebrauch von Cyberkapazitäten, um ermächtigende, störende oder zerstörende militante Operationen durchzuführen und Angst mittels Gewalt oder Gewaltandrohung zu instrumentalisieren, um einen politischen Wandel zu verfolgen*“.[37]

Angriffsziele von Cyberterroristen können kritische Infrastrukturen sein, wie beispielsweise Energie- und Wasserversorgung, Telekommunikation oder Verkehrs- und Transportsysteme, die bei Ausfällen zu erheblichen Beeinträchtigungen der öffentlichen Sicherheit oder zu Versorgungsengpässen oder anderen dramatischen Konsequenzen führen können.

Cyberterroristen nutzen das Internet nicht nur, um Anschläge zu verüben, sondern auch um neue, vor allem junge Mitstreiter zu rekrutieren sowie als Propagandawerkzeug oder zur Radikalisierung von Jugendlichen.

---

[36] Denning, D. E. (2001). *Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy*. In: Arquilla, J.; Ronfeldt, D. (eds.): *Networks and netwars: the future of terror, crime, and militancy*. RAND: National Defense Research Institute
Held, W.V. (2012). *Hacktivism: an Analysis of the Motive to Disseminate Confidential Information*. Im Internet: https://digital.library.txstate.edu/handle/10877/4381

[37] Brickey, J. (2012). *Defining Cyberterrorism: Capturing a Broad Range of Activities in Cyberspace*. Im Internet: http://www.ctc.usma.edu/posts/defining-cyberterrorism-capturing-a-broad-range-of-activities-in-cyberspace

4.1.3 Internetaktivismus

Internetaktivisten[38] setzen sich in erster Linie mit den Mitteln des Internets für das Internet ein. Das Internet und soziale Medien werden von Aktivisten als Diskussions-, Kommunikations- und Informationsmittel, z. B. bei der Mobilisierung von Anhängern oder der Planung von Aktionen, genutzt. Es gibt keine Angriffsziele im Netz, so dass auch keine Hacking- und IuK-Tools zur Begehung bspw. von Web-Defacements oder DDoS-Angriffe als Protestmittel eingesetzt werden.

Netzpolitische Aktivisten fordern eine demokratische Gestaltung und Nutzung des Internets. Es geht um einen gleichberechtigten Zugang zum Netz, um den Kampf gegen Zensur und um die Urheberrechtsproblematik.
Friedensaktivisten nutzen das weltweite Netz, um Sympathisanten zu mobilisieren, eine kollektive Identität zu schaffen oder als Informationsquelle. Carty und Onyett (2006) beschreiben das Vorgehen einer solchen Aktivistengruppe namens ANSWER[39], die sich unmittelbar nach den Anschlägen vom 11. September 2001 formierte.[40]
Brunsting und Postmes (2002) untersuchten anhand von Fragebögen 738 niederländische Umweltaktivisten und die Rolle, die das Internet bei der Planung und Durchführung kollektiver Aktionen spielt.[41] Vor allem die Möglichkeiten des Internets als eine Plattform für Massenkommunikation und Massenmobilisierung kristallisierten sich als neues Potential für den Aktivismus heraus.

Juris schildert die verschiedenen technischen Möglichkeiten, die Aktivisten nutzen. So können die Aktivisten via Internet Echtzeitnachrichten verbreiten, Interviews geben, Video- und Audioclips weitergeben oder das Vorgehen von Polizei und Sicherheitskräften mittels digitalen Filmmaterials festhalten. Er spricht in diesem Zusammenhang von „Media Activists“ oder „Video Activists“, die Internetplattformen wie z. B. Indymedia zur unabhängigen Berichterstattung nutzen.[42]

---

[38] auch Cyberaktivisten oder Medienaktivisten
[39] Act Now to Stop War & End Racism
[40] Carty, V./Onyett, J. (2006). *Protest, Cyberactivism and New Social Movements: the Reemergence of the Peace Movement Post 9/11*. In: Social Movement Studies, Vol. 5, 3, S. 229-249
[41] Brunsting, S./Postmes, T. (2002). *Social Movement Participation in the Digital Age: Predicting Offline and Online Collective Action.* In: Small Group Research 33: 525
[42] Juris, J. S. (2005). The New Digital Media and Activist Networking within Anti-Corporate Globalization Movements. In: The Annals of the American Academy. AAPSS, 597, S. 189-208

Denning beschreibt fünf Möglichkeiten, wie Aktivisten die Macht des Internets nutzen können:

1. *Collection*: die Sammlung von Informationen, bzw. die Nutzung des Internets als Bibliothek;
2. *Publication*: die Möglichkeit mit Hilfe des Internets als Massenmedium, Informationen zu verbreiten;
3. *Dialogue*: Austausch und Kommunikation mittels E-Mail, Web-Foren, Chatrooms etc.;
4. *Coordination of Action*: die Nutzung des Internets zur weltweiten Koordination und Planung von Aktionen sowie zur Mobilisierung von Aktivisten;
5. *Lobbying Decisionmakers*: die Möglichkeiten des Internets (z.B. Internetpetitionen, E-Maillisten) zu nutzen, um Entscheidungsträger für die eigene Sache zu überzeugen.[43]

Die Übergänge des Internetaktivismus hin zum Hacktivismus sind mitunter fließend.

4.1.4 Cyberkriminelle jenseits von politischen oder sozialen Motiven

Bei Cybercrime jenseits ideologischer Motive handelt es sich um die Verwirklichung von Straftaten im Internet in erster Linie zu Zwecken des (persönlichen) Profits. Darunter fallen Straftaten, die mit dem Hilfsmittel Internet begangen werden und zur Bereicherung einzelner oder Banden von Kriminellen dienen. Zu den Methoden der „allgemeinen" Cyberkriminellen gehören das Erschleichen von Informationen und (Zugangs-)Daten sowie der Diebstahl digitaler Identitäten mittels Social Engineering und Phishing. Gestohlene Daten und Identitäten werden u. a. für betrügerische Finanztransaktionen missbraucht oder aber als erpresserisches Mittel eingesetzt. Sabotage von und Angriffe auf Server und Webseiten, Cybermobbing, Cyberstalking, Cybergrooming sowie der Besitz und das Verbreiten illegalen Materials im Internet, wie z.B. Kinderpornographie und Raubkopien, zählen ebenfalls zur allgemeinen Cybercrime.

[43] Denning 2011

4.1.5 Cyberkriegsführung

Neben den bisher dargestellten Phänomenen muss das Phänomen Cyberwar bzw. Cyberkrieg ebenfalls von Hacktivismus abgegrenzt werden. Hierbei handelt es sich um die Nutzung des Internets und von Computern zur staatlichen Kriegsführung häufig im Sinne von Attacken oder Spionageangriffen. Mindestens eine der beteiligten Parteien muss zudem eine offizielle Regierung sein.[44]

Als einer der ersten Cyberkriege wird der Kosovokonflikt gesehen, in welchem die Beteiligten Informations- und Kommunikationstechnologien (IuK-Technologien) als Kampfmittel einsetzten. So wurde das jugoslawische Telefonnetz gestört und Konten des serbischen Präsidenten Milosevic gehackt, im Gegenzug störten serbische Hacker u. a. einen NATO-Server.
In einem weiteren Fall von Cyberwar griffen chinesische Hacker US-Regierungsseiten an, nachdem die chinesische Botschaft in Belgrad bombardiert wurde, und brachten sogar die Webseite des Weißen Hauses zum Erliegen.[45]

Neben tatsächlichen Kriegsschauplätzen können auch staatlich unterstützte Industriespionage und -sabotage unter den Begriff der Cyberwarfare subsumiert werden.
Die Autoren des Mandiant-APT-Reports 2013[46] glauben nachweisen zu können, dass die Angriffe von chinesischen Hackern auf ausländische Firmen, deren Daten ausspioniert und gestohlen wurden, von der chinesischen Regierung beauftragt und unterstützt wurden.
Im Kaspersky Security Bulletin 2012 wird von einer umfassenden Cyberspionage-Kampagne mit Namen ‚Flame', einer hochkomplexen Malware, sowie von dem Trojaner ‚Gauss' berichtet, die zusammen „*das Schlachtfeld Mittlerer Osten um eine neue Dimension erweitert: Cyberkrieg und Cyberkriegsführung*"[47].
Von gezielten Spionage-Angriffen chinesischer Hacker im Auftrag der Regierung Chinas auf die Computernetzwerke des US-Militärs berichtete im Mai 2013 SpiegelOnline.[48]

---

[44] Brenner, S.W. (2007). *„At Light Speed": Attribution and Response to Cybercrime/Terrorism/Warfare*. In: The Journal of Law & Criminology. Vol. 97 (2). S. 379-475
[45] Goel, S. (2011). *Cyberwarfare: Connecting the Dots in Cyber Intelligence*. In: Communications of the ACM. Vol. 54 (8). S. 132-140
[46] Advanced Persistant Threat
[47] Raiu, C. et al. (2012). *Kasparsky Security Bulletin 2012*. Im Internet: http://www.kaspersky.com/de/downloads/doc/kaspersky-security-bulletin-2012.pdf
[48] SpiegelOnline. (2013). *Chinas Hacker spähen US-Militär aus*. Im Internet: http://www.spiegel.de/politik/ausland/hackerangriffe-usa-beschuldigen-china-der-cyber-spionage-a-898446.html

4.2 Phänomenologie

4.2.1 Modi operandi

Die Vorgehensweisen der Hacktivisten variieren, abhängig von den zur Verfügung stehenden Mitteln (wie z. B. Online- und Hacking-Tools, aber auch Geld zur Beschaffung entsprechender Tools[49]), den technologischen Fähigkeiten der Hacktivisten, dem Zielobjekt und der Motivation bzw. der Ideologie (und des beabsichtigten Schadens).

Bei der Vorgehensweise von Hacktivisten lässt sich zum einen von organisatorisch-logistischen Vorbereitungshandlungen und zum anderen von der eigentlichen Tathandlung sprechen: Online-Tools und IuK-Technologien werden von Hacktivisten zur Planung entsprechender Aktivitäten verwendet. Über (Chat-) Foren, IRC[50], Twitter, Facebook usw. findet die Kommunikation und Logistik statt, d. h. Aktionen werden geplant und verabredet, Sympathisanten werden geworben und zur Teilnahme an Aktionen aufgerufen.

Unter der eigentlichen Tathandlung bzw. Vorgehensweise werden insbesondere Onlineaktivitäten verstanden, die die IT des Ziels manipulieren oder beschädigen sollen. Neben verschiedenen Angriffstechniken zählen hierzu auch Ausspäh- und Verschleierungstechniken im Sinne einer Anonymisierung des Angreifers.

In den letzten Jahren wurden überwiegend folgende Angriffstechniken von Hacktivisten genutzt:[51]

Site Defacements

Site Defacement, Web-Graffiti oder auch Web-Defacement meint das Verändern von Webseiten, indem entweder vorhandene Inhalte gelöscht oder aber durch neue ersetzt werden. Web-Defacements werden häufig eingesetzt, um Protest- und Propagandabotschaften auf Webseiten zu platzieren. Teilweise werden diese Botschaften wahllos auf Webseiten platziert, häufig werden z. B. Seiten von Unternehmen oder Regierungen und Parteien entsprechend der Ideologie und Zielsetzung der Hacktivisten gezielt angegriffen und inhaltlich manipuliert. In beiden Fällen dienen

[49] Im sog. Darkweb lassen sich neben Nutzerdaten, Exploits und sonstiger Schadsoftware auch Botnetze und DDoS-Angriffe erwerben.

[50] Internet Relay Chat

[51] U. a. Bundesamt für Sicherheit in der Informationstechnik. (2012). Register aktueller Cyber-Gefährdungen und
-Angriffsformen
Gragido, W./ Pirc, J. (2011). *Cybercrime and Espionage. An analysis of Subversive Multivector Threats*. Elsevier monographs. Amsterdam

die Defacements dazu, mit den Botschaften eine breite Öffentlichkeit zu erreichen. Daneben dienen sie auch der Einschränkung von webbasierten Dienst- und Serviceleistungen der angegriffenen Opfer.[52] Auch das wahllose Streuen von automatisierten Web-Defacements[53] zur vielfältigen Verbreitung von Botschaften und zu Übungszwecken wird von Hacktivisten (aber auch Hackern) genutzt.
Zone-h ist z. B. eine Webseite, auf der erfolgreiche Defacements mittels gespiegelten Seiten dokumentiert werden.[54] So können z. B. Hacker ihre Defacements beweisen und je nach Schwierigkeit und Herausforderung des Defacements Anerkennung von der Community erlangen.

Site Redirects

Bei Site Redirects wird der Besucher einer Webseite auf eine andere Seite umgelenkt. In den meisten Fällen handelt es sich hierbei um Seiten, die Protest- oder Propagandabotschaften zum Inhalt haben und sich häufig gegen die Intention/Inhalte/Zielrichtung der Ursprungsseite richten.
Der Hacktivist erlangt Kontrolle über die Nutzung der Ursprungsseite und kann die Besucher auf eigene Inhalte unter der scheinbaren Zieladresse umleiten.

Blockadetechniken (DDoS-Angriffe/Botnetze/SQL-Injection)

Mit einer virtuellen Blockade wird die Erreichbarkeit einer Webseite eingeschränkt bzw. vollständig verhindert. Bereits in der Vergangenheit konnte mittels E-Mail-Bomben[55] die Kommunikation eines Servers gestört werden. Bei DoS-Attacken[56] wird ein Server solange mit Anfragen bombardiert, bis seine maximale Kapazität zur Verarbeitung der Daten erreicht ist und der Server nicht mehr oder nur noch extrem langsam auf die Anfragen reagieren kann. Wird dieser Zusammenbruch durch ein ganzes Computernetzwerk hervorgerufen, spricht man von einem DDoS-Angriff[57].
Ein Botnetz entsteht, wenn zahlreiche Computer mit entsprechender Schadsoftware infiziert werden, welche einem Command and Control Server (C&C-Server) die Kontrolle über diese Rechner ermöglichen. Der C&C-Server schließt die infizierten Rechner, sog. Zombie-Rechner, zu einem Netzwerk zusammen und leitet Befehle an diese weiter. So lassen sich ohne das Wissen der Computerbesitzer z. B. DDoS-Angriffe steuern oder aber auch Spam-Mails und (illegale) Inhalte

[52] Z. B. Online-Handel, Banken, Informationsplattformen etc.
[53] Es ist möglich mittels Programmen Webseiten automatisch nach Sicherheitslücken abtasten zu lassen, um dann auf entsprechend ungeschützten Seiten Web-Defacements automatisch zu platzieren
[54] http://www.zone-h.org
[55] Massenhaftes Verschicken von E-Mails an eine Empfängeradresse bzw. Adressen einer Domain.
[56] Denial-of-Service-Attacken
[57] Distributed-Denial-of-Service-Angriff

weiterverbreiten. Cole et al. (2011) warnen vor den technischen Möglichkeiten, auch Smartphones für die Integration in ein Botnetz zu missbrauchen.[58]

Eine weitere Blockadetechnik ist das Ausspähen und Nutzen von Fehlern in der Datenbank-Software des Zielservers (z. B. mittels SQL-Injection), um diesen dann mittels unautorisierter Aktionen zu attackieren und lahmzulegen.

Je nach Fähigkeiten und Absichten werden diese Blockadetechniken auch von Hacktivisten genutzt. Hier überwiegt jedoch deutlich der Einsatz von DDoS-Angriffen, da sich diese relativ leicht und ohne zeitlichen Aufwand bewerkstelligen lassen. Das Erstellen eines Botnetzes ist aufwendiger oder aber teuer, wenn man dieses über das Darkweb bezieht. Über die Nutzung von SQL-Injections durch Hacktivisten ist bislang wenig bekannt.

Virtuelle Sit-Ins

Diese Form des Hacktivismus gleicht dem DDoS-Angriff über ein Botnetz, jedoch mit dem Unterschied, dass das Netzwerk, von welchem die Anfragen an den Zielserver geschickt werden, aus Computern besteht, die von den Nutzern freiwillig zur Verfügung gestellt werden. Entweder werden die Anfragen manuell oder automatisiert über spezielle Software wie z. B. LOIC[59].ausgeführt. Virtuelle Sit-Ins werden von verschiedenen Autoren als eine verbreitete demokratische und repräsentative Form des Hacktivismus betrachtet.[60]

Sabotage

Mittels Hacking-Tools wird bei einer Sabotage Aktion die Informationstechnologie des Ziels manipuliert, beschädigt oder zerstört. Schadsoftware wie Viren, Trojaner und Exploits können auch von Hacktivisten zu Sabotagezwecken eingesetzt werden, erfordern jedoch den Zugang zu solchen Programmen und entsprechende Fähigkeiten in der Anwendung oder der Entwicklung dieser Software.

---

[58] Cole, K. A. et al. (2011). *All Bot Net: A Need for Smartphone P2P Awareness*. In: P. Gladyshv, M.K. Rogers. (Hrsg.): *Digital Forensics and Cyber Crime*. Third International ICST Conference ICDF2C 2011, Dublin, Ireland, revised Selected Papers. S. 36-46

[59] Low Orbit Ion Canon

[60] U. a. Fitri, N. (2011). *Democracy Discourses through the Internet Communication: Understanding the Hacktivism for the global Changing*. In: Online Journal of Communication and Media Technologies Volume: 1 – Issue: 2 – April – 2011

Kelly, B.B. (2012). *Investing in a Centralized Cybersecurity Infrastructure: Why „Hacktivism" can and should influence Cybersecurity Reform*. In: Boston University Law Review. Vol. S. 92. 1663-1711

O`Rourke, S. (2011). *Empowering Protest through Social Media*. Published by:School of Computer and Information Science, Security Research Centre, Edith Cowan University, Perth, Western Australia

Softwareentwicklung (als mögliches Hilfsmittel)

Wie bereits erwähnt entwickeln informationstechnisch begabte Hacktivisten eigene Tools und Programme, die im Rahmen hacktivistischer Zielrichtungen unterschiedliche Anwendungen finden.

Beispiele hierfür sind u. a. die Entwicklung von Programmen, die es dem Nutzer ermöglichen (z. B. durch Regierungen) zensierte und blockierte Seiten zu besuchen sowie Software, die zur Einrichtung und Umsetzung von DDoS-Angriffen dient. Eigene entwickelte Programme werden oft im Netz für die freie Nutzung und Weiterentwicklung zur Verfügung gestellt.

Gefälschte Seiten

Bei gefälschten Seiten oder Seiten-Parodien handelt es sich um der Zielseite ähnliche, aber durch Parodien veränderte Webseiten, die eine der ursprünglichen sehr ähnliche URL verwenden und somit von Nutzern versehentlich besucht werden. Auch dies ist ein Weg, Protest- und Propagandabotschaften zu verbreiten. Diese Art des Hacktivismus wird auch mit der Untergrundpresse des Aktivismus verglichen.[61]

Doxing

Doxing oder d0xing ist die Abkürzung für „document tracing". Dabei werden (intime) Daten einer Person über das Internet gesammelt bzw. ausgespäht und veröffentlicht. Bei diesen Daten kann es sich um alles handeln, was durch Recherchen auf sozialen Plattformen, in Datenbanken oder aber auch durch Hacking und Social Engineering zusammengestellt werden konnte, wie z. B. Namen, (digitale und analoge) Adressen, Fotos, Angaben zur Familie, zu Hobbies, Vorlieben u. s. w.

Motivationen für das Doxing sind z. B. Outing von Kriminellen, Erpressung und Selbstjustiz. Im Bereich des Hacktivismus steht vor allem das Outing und Schlechtmachen von ideologisch und politisch Andersdenkenden bzw. ideologischen Gegnern im Vordergrund.

Datendiebstahl und Ausspähtechniken

Beim Ausspähen von Daten werden Zugänge zu Konten, sozialen Netzwerken, Computern und Systemen gehackt. Beim Hacktivismus werden die so erlangten Daten z. B. im Rahmen des Doxing missbraucht.[62]

---

[61] Alleyne, B. (2011). *We are all hackers now - critical sociological reflections on the hacking phenomenon*. In: Under Review, 1-28

[62] Der Missbrauch solcher Daten zur Profiterzielung entspricht nicht mehr der Definition von Hacktivismus und fällt unter das Phänomen *Cybercrime jenseits von politischen oder sozialen Motiven.*

Zu den Ausspähtechniken zählen der Einsatz von Schadsoftware und das Social Engineering. Während das Ausspähen mittels Schadsoftware rein informationstechnologisch erfolgt,[63] nutzt das Social Engineering die soziale Komponente der Beeinflussung einer Zielperson zur Preisgabe relevanter Informationen. Diese Informationen dienen dann dem Zugang zu Konten oder Systemen oder aber auch zur Installation von Schadsoftware und dem folgenden Ausspähen von Daten.[64]

Verschleierungstechniken

Um im Cyberraum unerkannt und unbeobachtet agieren zu können, nutzen insbesondere Cyberkriminelle Anonymisierungsmöglichkeiten. Mittels TOR[65] wird der Internetdatenverkehr über mehrere Server-Knotenpunkte geleitet, um die Ermittlung der IP-Adresse zu erschweren bzw. unmöglich zu machen. Weitere Möglichkeiten, unerkannt im Internet zu agieren, bestehen in der Nutzung von Internetcafés, WLAN-Verbindungen in Hotels, WLAN Hot Spots oder in der missbräuchlichen Nutzung der WLAN-Verbindungen anderer Personen bzw. Institutionen.
Neben TOR bietet z. B. I2P[66] eine technische Lösung zur anonymen Kommunikation im Internet mittels End-to-End-Kryptierung. Auch das Six/Four System, das wie ein verschlüsselter Tunnel zwischen zwei Computern funktioniert, wird zur sicheren Kommunikation verwendet.

[63] Malware installiert sich von den Nutzern unbemerkt auf deren Rechnern und späht Daten nicht nur aus, sondern kann diese auch verändern und zerstören. Vor allem Zugangsdaten, Bankdaten, Benutzernamen und Passwörter sind das Ziel solcher Spionagesoftware. Eingeschleust wird Malware überwiegend über infizierte E-Mail-Anhänge, Drive-by-Infections oder aus dem Internet heruntergeladene Dateien.
[64] Kochheim, D. (2010). *Cybercrime -Malware, Social Engineering, Underground Economy*. Im Internet: http://www.kochheim.de/cf/doc/Cybercrime-2010.pdf
[65] The Onion Router
[66] Invisible Internet Project

In den von Held ausgewerteten Pressemitteilungen fanden sich die in Abbildung 10 dargestellten prozentualen Anteile an Hackerangriffstechniken[67]:

Category	Frequency	Percent
Act: Website Defacement	30	26.5%
Act: Server Intrusion	27	23.9%
Act: Data Wiped	20	17.7%
Act: Sever Map/Configuration	9	8.0%
Act: Restraint	9	8.0%
Act: Website Offline	6	5.3%
Act: Network Take Over	5	4.4%
Act: Website Intrusion	4	3.5%
Act: Chat Logs Posted	3	2.7%
Total	**113**	**100%**

Abbildung 8: Vorgehensweisen. Held, W.V. (2012). Hacktivism: an Analysis of the Motive to Disseminate Confidential Information. – Vorgehensweisen

Es ist ersichtlich, dass Web-Defacements, das Eindringen in Server und das Manipulieren und Zerstören von Daten mit insgesamt 68,1 % den Schwerpunkt in den genutzten Vorgehensweisen ausmachen.

Ein ähnliches Bild liefern auch die Ergebnisse der Fallanalyse (s. Abbildung 11): Die Fälle, in denen Web-Defacements genutzt wurden, überwiegen mit 59 % (46 Fälle) alle anderen Vorgehensweisen. In 21,8 % der Fälle wurden Daten ausgespäht und in 10,3 % der Fälle wurden Daten verändert bzw. gelöscht. DDoS-Angriffe machten lediglich 5,1 % aus (4 Fälle), wobei zu berücksichtigen ist, dass das Feststellen eines DDoS-Angriffs ggf. schwieriger sein kann als das Bemerken eines Web-Defacements und hierbei auch das Beweismaterial für DDoS-Angriffe für den Geschädigten schwieriger festzuhalten ist. Dies könnten u. a. Gründe sein, warum DDoS-Angriffe seltener zur Anzeige gebracht werden als Defacements und damit statistisch im Hellfeld seltener auftauchen.

[67] Held 2012

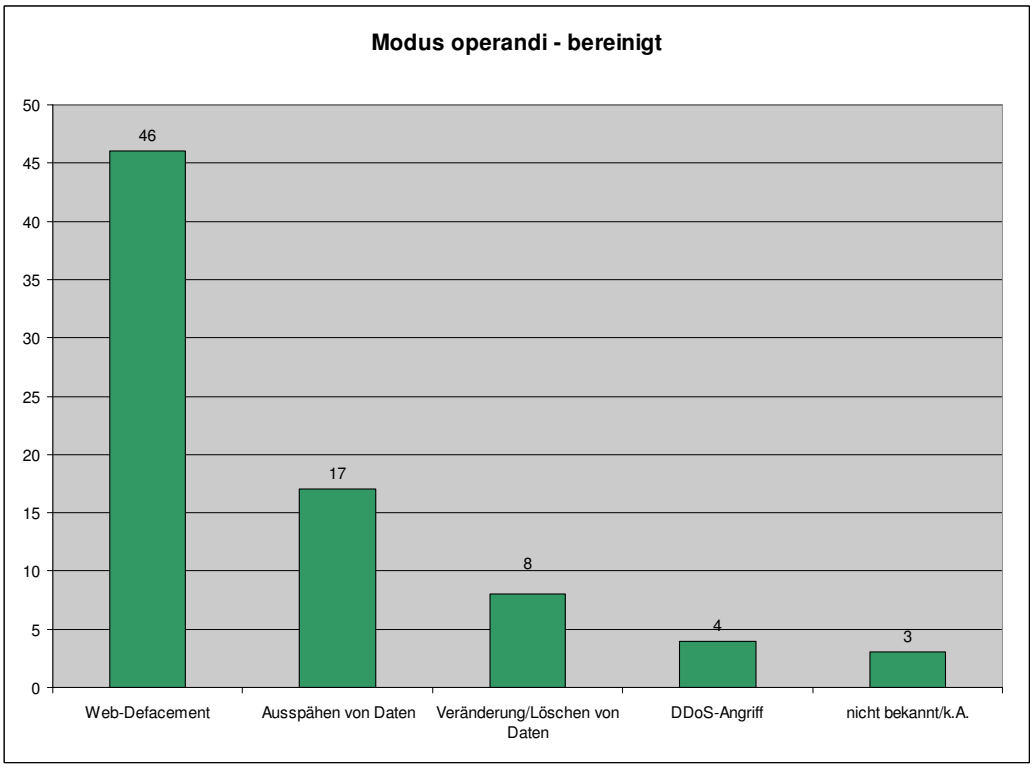


Abbildung 9: Darstellung der Vorgehensweise bei 78 Fällen.

Strafbarkeit

In der Fallanalyse wurde zudem überprüft, welche Vorgehensweise unter welchem Straftatbestand subsumiert und erfasst wurde (s. Abbildung 12). Web-Defacements fielen hier – ebenso wie DDoS-Angriffe – insbesondere unter § 303 a StGB (Datenveränderung). Das Ausspähen von Daten wurde überwiegend unter § 303 b StGB (Computersabotage) eingeordnet, aber auch unter § 202 a StGB (Ausspähen von Daten) sowie unter § 202 b StGB (Abfangen von Daten) und § 43 II 2,3 BDSG (Ordnungswidrigkeit personenbezogene Daten ausspähen/bereithalten). Das Verändern und Löschen von Daten wurde in einem Fall unter § 303 a StGB (Datenveränderung) und in einem anderen Fall unter § 303 b StGB (Computersabotage) gestellt.

Die Einstufung der Vorgehensweise in Strafnormen des StGB oblag in erster Linie dem Sachbearbeiter.

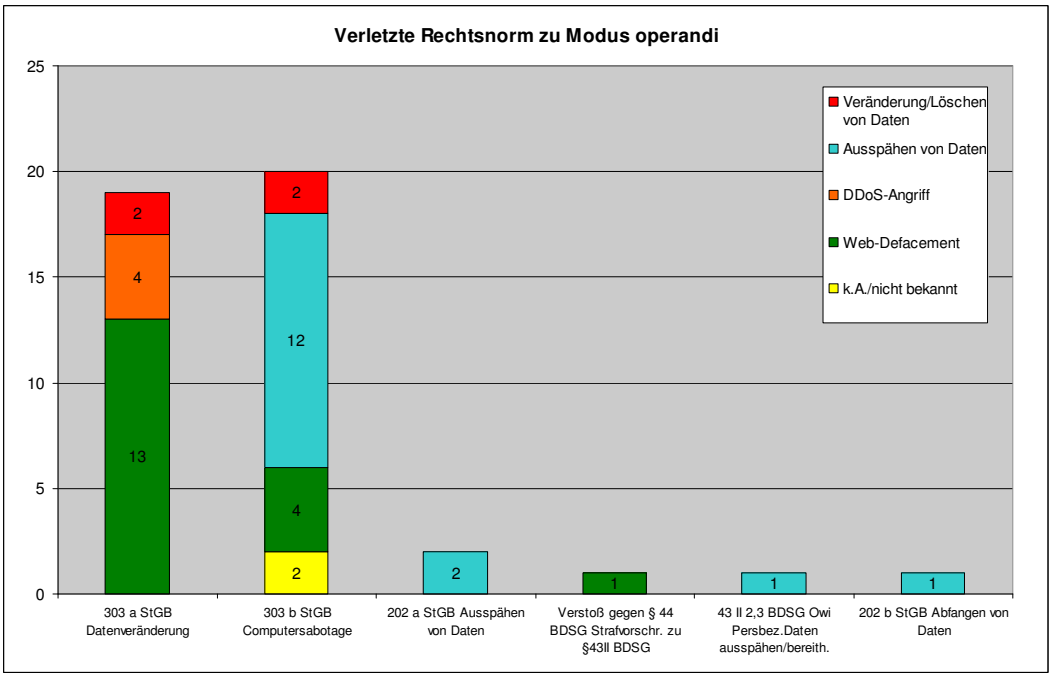


Abbildung 80: Darstellung des angewendeten Straftatbestands bei 78 Fällen.

4.2.2 Infrastruktur

Um hacktivistische Aktionen zu planen und durchzuführen sowie Sympathisanten zu mobilisieren, müssen logistische Probleme wie Kommunikation oder Timing gelöst werden.
Auch wenn es hier kein einheitliches Vorgehen unter den verschiedenen hacktivistischen Gruppierungen gibt, so lassen sich aus der Analyse der Anonymous-Gruppierung[68] beispielhaft Rückschlüsse auf die Infrastrukur hacktivistischer Gruppierungen ziehen.[69]

Ein einigermaßen stabiles Kommunikationsnetzwerk ist Voraussetzung für die Zusammenarbeit jeglicher Gruppierungen, die über das Internet agieren. Der Großteil der von Samuel (2004) befragten Hacktivisten gab an, dass sie untereinander in regem Kontakt stünden und regelmäßig kommunizieren würden. Die Kommunikation von Anonymous (und auch von anderen Gruppen) wird über einen breiten Zugang von Kommunikationskanälen dezentralisiert, wie z.B.

[68] Letztlich ist die Wortwahl Gruppierung nicht ganz richtig, da es sich bei Anonymous (wie auch bei anderen hacktivistischen Gruppierungen) vielmehr um anlassbezogene Zusammenschlüsse von anonymen Personen unter dem Pseudonym Anonymous handelt.
[69] Anonymous bietet sich hier insbesondere deshalb an, da hier im Vergleich zu anderen hacktivistischen Gruppierungen entsprechend auswertbares Material vorliegt und Anonymous bislang auch in der Literatur am meisten Aufmerksamkeit erfahren hat und hier entsprechende Erkenntnisse vorliegen.

Imageboards, Chatrooms, Blogs, soziale Netzwerke wie Twitter oder Facebook, Mailinglisten oder IRC-Kanälen. [70]

Nach eigenen Aussagen von Anonymous-Mitgliedern[71] kann jeder Vorschläge zu Aktionen machen, über deren Umsetzung die Mitglieder dann abstimmen. Sind genügend Mitstreiter vorhanden, wird die Aktion geplant und umgesetzt. Für Vorschläge und Planungen wurde anfänglich die Plattform „4chan /b/" genutzt. Nachdem jedoch die Zahl der Mitstreiter, Neugierigen sowie Gegner in diesem Forum stetig stieg, wurden andere Kommunikationsplattformen gegründet. Eine dieser Plattformen ist AnonOps, auf der der Initiator einer Aktion einen IRC-Kanal öffnen kann, über welchen Planungen, Diskussionen und auch Anweisungen zur Vorgehensweise, wie z. B. zur Konfiguration der LOIC-Software, stattfindet.

Hacktivistische Gruppierungen sind grundsätzlich führerlos. Bei einzelnen Aktionen finden sich neben dem/n Initiator/en oft spontan „Zuständige" für bestimmte Aufgaben. Zum Beispiel fragte während des Projekts Chanology ein Anonymous-Mitglied, ob man nicht die Presse informieren solle. Daraufhin wurde unter einem neuen IRC-Kanal eine nicht-hierarchische Pressegruppe gebildet, die Pressemitteilungen verfasste und veröffentlichte.

4.2.3 Szene

Eine der ersten Hacktivistengruppen ist *Cult of the Dead Cow* (cDc), die als eine der ersten Gruppen mit dem Begriff „Hacktivismus" Mitte der 90er Jahre in Verbindung gebracht wurden. Die Gruppe setzt sich für einen weltweit ungehinderten und unzensierten Fluss an Informationen im Internet ein.[72] Mit der *Hacktivismo-Declaration*[73] erklärt die Gruppierung ihre Ablehnung staatlicher Zensur von kritischen, intellektuellen, künstlerischen und religiösen Inhalten im Internet. Die Hacktivismo-Declaration erklärt, dass die Mitglieder an „ *Mittel und Wegen arbeiten, staatliche Zensur am Internet zu umgehen und Techniken zu verbreiten, die das Informationsrecht verteidigen*"[74].

[70] Hearn, K./Mahncke, R./Williams, P.A. (2009). *Culture Jamming: From Activism to Hactivism*. ECU Publications
[71] Olson, P. (2012*). Inside Anonymous: Aus dem Innenleben des globalen Cyber-Aufstandes*. Redline Verlag. München.
[72] U. a. Jordan/Taylor 2004
Paget, F. (2012). *Hacktivismus-Das Internet ist das neue Medium für politische Stimmen.* Im Internet: http://www.mcafee.com/de/resources/white-papers/wp-hacktivism.pdf
[73] Hacktivismo ist ein Nebenzweig der cDc-Gruppe
[74] Fitri 2011, S. 10

Die Gruppe bewirkte u. a. mittels der Schadsoftware „Goolag", dass Öffentlichkeit und Medien zum einen die Anfälligkeiten von Webseiten wahrnahmen und legte zum anderen die Zensurpraktiken der chinesischen Regierung von Google offen.[75]

Eine weitere Hacktivistengruppe, die mit der neuen Form des elektronischen Protests vor allem gegen die mexikanische Regierung experimentierte, nannte sich *The Electronic Disturbance Theater* (EDT). Diese koordinierte eine Reihe von Web-Sit-Ins, um Regierungsgegner zu unterstützen. Dafür entwickelten die Gruppenmitglieder die FloodNet Software, mittels derer freiwillige Botnetzwerke aufgebaut werden können.[76]

Die *ElectroHippies*, eine britische Hacktivistengruppe, organisierte unter anderem einen Cyberprotest, der jeden dazu aufrief, die WTO Website wiederholt aufzurufen, um damit einen (D)DoS-Angriff auszulösen, der die Server der WTO Website zum Absturz bringt. Die Hacktivistengruppe *World´s Fantabulous Defacers* (WFD) formierte sich im November 2000 und startete eine zwei Jahre andauernde Serie von Web-Defacements im Rahmen des Pakistankonflikts.[77] 45 indonesische Webseiten wurden von dem *Kaotik Team* defaced, um für die volle Autonomie von Osttimor zu protestieren.[78]
Weitere Hacktivistengruppen, die sich gegen Krieg, Atomwaffen und für den Frieden einsetzen, sind das amerikanische Team *sp10it*, die während des Kosovokonflikts mit Web-Defacements aktiv wurden, die *Asthray Lumberjacks*, die sich in das britische Internetservice hackten und die *Wannabe Hacker*, ein junges indonesisches Hackerteam, das sich mit Palästina solidarisierte.[79]

Telecomix, eine 2009 in Schweden gegründete Gruppe mit 250-300 Mitgliedern ohne Hierarchie und nach dem Prinzip der „do-ocracy"[80] operierend, stellte beispielsweise 2011 den von der ägyptischen und lybischen Regierung gekappten Zugang zum Internet wieder her. Später verbreiteten sie eine Nachricht mit der Beschreibung zur Umgehung der Online-Überwachung an

---

[75] U. a. Hearn/Mahncke/Williams 2009
Fitri 2011
Samuel 2004
[76] U. a. Juris 2005
Taylor, P.A. (2005). *From Hackers to Hacktivists: speed bumps on the global highway*. In: New Media Society, 7, 625-646
[77] Samuel 2004
[78] metac0m. (2003). *What is Hacktivism? 2.0.* Im Internet: http://www.thehacktivist.com/hacktivism1.php
[79] U. a. Fitri 2011 und Denning 2001
[80] Do-ocracy ist eine Mischform aus dem englischen Do und Democracy und gibt an, dass Personen Aufgaben selbstständig wählen, diese ausführen und für diese auch selber die Verantwortung übernehmen.

die syrischen Internetnutzer.[81] 2010 gab die Gruppe *4ATA* (Fourth Awaking People´s Army) in Lettland bekannt, dass sie Zugriff auf Millionen lettischer Steuerdokumente habe. Einige Informationen daraus wurden veröffentlicht, um Korruptionsfälle aufzudecken.[82]

Neben den erwähnten Gruppierungen gibt es eine Vielzahl von weiteren hacktivistischen Gruppierungen und deren Splittergruppen sowie eine Masse von Hacker- und Hacktivistenangriffen, die keiner Gruppe eindeutig zugeordnet werden können. Eine besondere Rolle bei der Auswertung und Darstellung von Hacktivistengruppen spielt *Anonymous*, da zur Geschichte, Struktur und Vorgehensweise dieser Gruppe bereits umfassend geforscht wurde und diese Gruppe den Hacktivismus, seine Vielfalt und seine Ambivalenzen exemplarisch recht gut wiedergibt. Daher wird diese Gruppierung im Folgenden näher dargestellt.

Anonymous

Anonymous ist ein loser Zusammenschluss von Hackern und Hacktivisten, dessen Größe nicht fest, sondern abhängig von verschiedenen Faktoren wie z. B. gesellschaftlichen oder politischen Ereignissen an- und abschwellend ist. Daneben weist die Gruppierung – wie viele andere hacktivistische Gruppen auch – keine (ausgeprägte) hierarchische Führungsstruktur auf, kommunizierte Inhalte und Aktionen werden weder kontrolliert, zensiert noch moderiert.[83] Weitere Merkmale mit denen sich die Gruppe der Öffentlichkeit präsentiert, sind zum einen die Guy-Fawkes-Maske und zum anderen der Slogan: „*Anonymous is Legion. We do not Forgive. We do not Forget. Expect us.*“. Das Abbild der Maske sowie der Slogan werden u. a. für Pressemitteilungen, Inhalte von Web-Defacements und YouTube-Videos genutzt. Die Mitglieder der Gruppe nennen sich selber „Anons“.[84]

Abbildung 9: Von Anonymous genutzte Grafik.

[81] Vgl. Paget 2012
[82] ebd.
[83] U. a. McLaughlin, V. (2012). *Anonymous - What to fear from hacktivism, the lulz, and the hive mind?* Im Internet:
http://pages.shanti.virginia.edu/Victoria_McLaughlin/files/2012/04/McLaughlin_PST_Thesis_2012.pdf
Slobbe, J./Verberkt, S.L.C. (2012). *Hacktivists: Cyberterrorists or Online Activists? An Exploration of the Digital Right to Assembly*. In: CoRR abs/1208.4568
[84] Paget 2012

Gerade weil sich Anonymous aus einem losen Kollektiv ohne hierarchisch ausgeprägte Führungsstruktur und aus unterschiedlichsten Personen, die alle Stimmrecht besitzen, zusammensetzt, ist es sehr schwer die ideologischen Ziele auf einen Nenner zu bringen.
Ideologisch eint jedoch alle Anons die Forderung nach einem freien, unzensierten und zugänglichen Internet. Daneben werden verschiedene Aktionen u. a. gegen Rassismus, Nationalsozialismus, Scientology, Pädophilie, Strafverfolgungsorgane, Regierungen, Organisationen und Unternehmen, welche die Freiheitsrechte nach Ansicht der Anons in irgendeiner Art beeinträchtigten, geplant und umgesetzt.

Auf der Plattform „4chan" im Forum „/b/" begann die Entstehungsgeschichte von Anonymous. Wer dem Forum beitritt und keinen Nickname wählt, wird automatisch unter dem Namen „anonymous" geführt und postet unter diesem Namen auch seine Beiträge. Die Nutzer dieses Forums bezeichneten sich selbst als Internettrolle, die teilweise recht bösartige Späße (lulz) auf Kosten von unterschiedlichen Opfern im Internet begingen. Zunehmend wurden solche Aktivitäten verabredet und es entstand ein loses Kollektiv aus den Nutzern des „4chan/b/"-Forums, die den Namen nutzten, der ihnen dort zugeteilt wurde: Anonymous.[85]

Eine der ersten gemeinsamen Aktionen war 2006 der sogenannte „Habbo-Raid"[86], dann folgten teilweise sozialkritische Aktionen, wie der Angriff auf die Website des amerikanischen Nationalisten Hal Turner Ende 2006 oder Aktionen gegen einen pädophilen Kanadier, die dann schließlich in dessen Verhaftung endeten. In der 2008 gestarteten Aktion gegen Scientology[87] sehen viele einen Wendepunkt, an dem aus einer reinen Spaßgruppe eine politisch und sozial ausgerichtete Hacktivistengruppe wurde.

Im Laufe der Zeit gruppierten sich immer wieder Untersektionen von Anonymous, wie z. B. die Gruppe *LulzSec*. Im Gegensatz zu Anonymous weist diese Hacktivistengruppe eine Führungsstruktur auf. So war Kopf der LulzSec-Operationen eine Person mit dem Internetspitznamen Sabu. Führende Mitglieder waren Topiary (Operator der Public Relations der

[85] U. a. Held 2012
McLaughlin 2012
[86] Das Habbo-Hotel ist ein Online-Spiel, eine virtuelle Welt, bei dem sich der Besucher in Gestalt einer selbst gewählten Figur in einem virtuellen Hotel aufhalten kann. Anonymous-Mitglieder besetzten mit Avataren in Gestalt von Afroamerikanern in Anzügen den Pool und verweigerten damit anderen Spielern den Zugang. Neben einer reinen Spaßmotivation (for the lulz), wurde mit der Wahl von Afroamerikanern auch auf die Unterrepräsentation von Schwarzen in dieser virtuellen Welt aufmerksam gemacht und hatte somit auch eine soziale und politische Komponente (u.a. McLaughlin 2012; Paget 2012).
[87] Genannt „Chanology".

Gruppe), Kayla (Operator eines großen Bot-Netzwerks) und T-Flow (Programmierer und Operator der Website der Gruppe). Das oberste Ziel der Gruppe war der „Lulz" – also der Spaß am Hacken und die Schadenfreude, auch wenn einige Aktionen durchaus soziale und politische Aspekte hatten.

Am 19. Juli 2011 verhaftete das FBI sechzehn Mitglieder von Anonymous aus Kalifornien, New York, Florida und New Jersey. In London nahm die Polizei am selben Tag einen 16-Jährigen fest, von dem man glaubte, er sei T-Flow, ein offizielles Mitglied von LulzSec. Auch Sabu (Hector Xavier Monsegur), Kayla (Ryan Ackroyd), Topiary (Jack Davis) und weitere Mitglieder wurden im März 2012 verhaftet. Es stellte sich heraus, dass Sabu seit Juli 2011, als er das erste Mal verhaftet wurde, als Informant für das FBI arbeitete.

LulzSec operierte für eine kurze Dauer von 50 Tagen (genannt 50 Days of Lulz), von Mai bis Ende Juli 2011. In dieser Zeit erlangte LulzSec ein immenses Medieninteresse sowie Aufmerksamkeit der US Regierung. Mit dem Ende ihrer Aktivitäten half LulzSec dabei, die AntiSec-Bewegung zusammen mit Anonymous aufzubauen.[88]

AntiSec – von den gleichen Zielen und Wünschen motiviert, wie Anonymous und LulzSec –wurde vor allem darin aktiv, Hacks zu publizieren. Jeder, der hacktivistische Aktionen plante, wurde ermutigt, es unter dem Banner von AntiSec zu tun:

> „*Welcome to Operation Anti-Security (#AntiSec) we encourage any vessel, large or small, to open fire on any government or agency that crosses their path. We fully endorse the flaunting of the word "AntiSec" on any government website defacement or physical graffiti art. We encourage you to spread the word of AntiSec far and wide, for it will be remembered. To increase efforts, we are now teaming up with the Anonymous collective and all affiliated battleships.* "[89]

AntiSec wie auch LulzSec publizierten einen Großteil der Veröffentlichung auf der BitTorrent File Sharing Website „The Pirate Bay".

Murphy berichtete 2012 von einem neuen Ableger von Anonymous, der *MalSec* (Malicious Security), die sich wie ihre Vorgänger der Internetfreiheit und dem Kampf gegen Zensur verschrieben haben. Diverse Angriffe auf chinesische Regierungswebseiten, auf die des New Jersey Police Departments, sowie auf eine Sicherheitsfirma auf den Cayman Inseln werden dem

[88] Colemann, G. (2012). *Anonymous: Leuchtfeuer der digitalen Freiheit*. In: M. Beckedahl, A. Meister (Hrsg.). *Jahrbuch Netzpolitik 2012 – von A wie ACTA bis Z wie Zensur*. epubli GmbH, Berlin. S. 220-227

[89] Held 2012, S. 48

neuen Ableger von Anonymous zugeschrieben. MalSec wenden sich mit einem ethischen Vorgehen von dem Personenkult LulzSec's ab und orientieren sich damit wieder an dem ursprünglichen führerlosen Modell von Anonymous.

Die Führerlosigkeit von Anonymous birgt dabei auch Risiken für die Gruppe selbst. Da sich jeder anonym für Aktionen aussprechen und auf den Plattformen mitdiskutieren kann, ist es jederzeit möglich, dass Anonymous infiltriert wird: So können sich Vertreter polizeilicher oder geheimdienstlicher Seite ebenso wie hacktivistische Gegner als Anons ausgeben. Es können Bekennungen, Nachrichten und Gerüchte über und unter dem Namen der Gruppe verbreitet werden, die nicht zutreffen. So sollte z. B. die Gruppe Anonymous im Internet angekündigt haben, dass am 5. November 2011 das soziale Netzwerk Facebook wegen seiner Datenschutzmängel gekapert werden solle. Trotz vieler Dementis von Seiten Anonymous hielt sich das Gerücht bis zum 6. November, als Facebook nach wie vor funktionierte.

Umgekehrt wurde eine Aktion gegen das British Office for National Statistics, die unter dem Namen von LulzSec lief, später im LulzSec Twitter dementiert: „*That wasn´t us – don´t believe fake LulzSec releases unless we put out a tweet first.*"[90]

Auch gibt es Gerüchte, dass das FBI selbst am „Stratfor Hack"[91] beteiligt gewesen sei. Solche Legenden halten sich umso hartnäckiger, seit bekannt wurde, dass Sabu, ehemaliger Kopf von LulzSec, mit dem FBI zusammenarbeitete.[92]

4.2.4 Geschädigte und Schäden

Die angegriffenen Ziele von Hacktivisten sind abhängig von der jeweiligen ideologischen Ausrichtung der Gruppe (oder des Einzeltäters) bzw. von den gewählten Operationen (im Kontext gesellschaftlicher und politischer Ereignisse).

Held hat unterschiedliche Kategorien in seiner Beforschung von Hacktivisten herausgefunden, die sich zwar auf die Motivation beziehen, jedoch Aussagen zu Zielobjekten zulassen:[93]

[90] Held 2012, S. 51

[91] Das Sicherheitsberatungsunternehmen Stratfor, das unter anderem für das Pentagon, Rüstungsfirmen, Ölkonzerne, Versicherungen und Banken arbeitet, wurde im Dezember 2011 zum Ziel eines großangelegten Angriffs. Der nachlässige Umgang mit unverschlüsselten Kundendaten ermöglichte es AntiSec über 860.000 E-Mail- Zugangsdaten und über 75.000 Kreditkartennummern zu stehlen. Die Startseite von Stratfor wurde defaced und interne E-Mails bei WikiLeaks im Februar 2012 veröffentlicht (Reitmann, J. (2012). *Enemy ofthe State*. In: Rolling Stone, Issue 1169, S. 52-62).

[92] McLaughlin 2012

[93] Held 2012

Category	Frequency	Percent
Motivation: Anti Police	175	40.0%
Motivation: Anti Government	103	23.6%
Motivation: Anti Corporation	58	13.3%
Motivation: Electronic Civil Disobedience	32	7.3%
Motivation: Anti Military	24	5.5%
Motivation: Anti FBI / CIA	24	5.5%
Motivation: Anti Banks	10	2.3%
Motivation: Anti Media	6	1.4%
Motivation: Anti Politics	4	0.9%
Motivation: Pro Investigative Journalism	1	0.2%
Total	**437**	**100%**

Abbildung 10: Hacktivistische Zielrichtungen. Held, W.V. (2012). Hacktivism: an Analysis of the Motive to Disseminate Confidential Information.

Anhand der Auswertung von Held ist ersichtlich, dass sich die Motivation von Hacktivisten überwiegend gegen die Polizei, gegen die Regierung und gegen Unternehmen richtet. Daher ist davon auszugehen, dass die genannten auch in erster Linie Zielobjekte hacktivistischer Aktivitäten darstellen.

Diese Tatsache entspricht auch anderen Erkenntnissen aus der Literatur: Regierungen und deren politische Vertreter oder staatliche Organe sind immer wieder im Zielspektrum von Hacktivisten.[94] Zum einen werden Regierungen attackiert, weil sie aus Sicht der Hacktivisten gegen Menschenrechte verstoßen oder das Internet zensieren, zum anderen werden sie attackiert, weil die Internetfreiheit den Aktivisten nicht weit genug reicht. Außerdem sollen Missstände im Datenschutz aufgezeigt und dagegen protestiert werden.

[94] Arns, I. (2002). *Netzkulturen*. Europäische Verlagsanstalt. Hamburg.
Denning 2001
Jordan, T. (2001). *Mapping Hacktivism*. In: *Computer fraud & security*, 4, 8-11
Jordan/Taylor 2004

Im Folgenden werden einzelne Beispiele aufgeführt, die einen Überblick über vergangene Angriffe auf staatliche Organe geben sollen:

- Die NASA wurde 1988 von Aktivisten aus Protest gegen Atomtest mit dem Computerwurm WANK[95] infiziert.
- Polizeibeamte der US-amerikanischen Polizei-Departements werden immer wieder Ziel von Doxing-Angriffen.
- Polizisten in Brasilien und Ecuador wurden Opfer von Doxing-Angriffen.
- DDoS-Angriffe gegen Server der britischen Regierung wurden als Protest für ein Verbot von „eintönigen" Konzerten im Freien gestartet (1994).
- Italienische Hacktivisten attackierten 1995 französische Webseiten aus Protest gegen die Mururoa-Atoll-Atomtests.
- Portugiesische Hacktivisten protestierten 1997 mit Angriffen auf indonesische Regierungsseiten gegen die Unterdrückung des Volkes.
- Mexikanische Webseiten werden seit 1998 von Pro-Zapatista-Hackern/Hacktivisten angegriffen.
- Zensurpläne der türkischen Regierung riefen Hacktivisten auf den Plan (2011).
- Doxing-Angriffe gegen Polizisten in Österreich und Frankreich.
- Nachdem die Regierung Polens das ACTA unterstützen wollte, wurden Regierungsseiten 2012 mit DDoS-Attacken angegriffen.

Neben Regierungen sind auch Firmen, Banken und Konzerne immer wieder im Fokus von Hacktivisten. Im Folgenden werden einige populäre Beispiele hacktivistischer Angriffe auf die Wirtschaft genannt:[96]

- 1999 begann der Widerstand gegen eToy Inc., eine Internetspielzeugversandfirma, die gegen eine Gruppe von Schweizer Künstlern (etoy) vorging, deren Domainname mit dem Unternehmensnamen übereinstimmte, aber schon seit Jahren existierte. eToy Inc. setzten ihre Interessen vor Gericht durch. Daraufhin reagierten Hacktivisten und erreichten durch die Blockade der Webseite der Firma einen Einbruch des Aktienkurses. Ende Januar ließ eToys.com die Klage gegen die Künstlergruppe fallen, „nicht zuletzt

[95] Worm Against Nuclear Killers
[96] Jordan/Taylor 2004

wegen der heftigen Gegenreaktionen, die eToys.com zu spüren bekommen hatte."[97] Diese Aktion wurde unter dem Namen Toywar bekannt.

- Ein virtueller Protest aus Deutschland legte 2001 die Website von Lufthansa lahm. Die Aktion richtete sich gegen die Abschiebung illegaler Immigranten in Lufthansa-Maschinen.
- Umwelt-Hacktivisten protestieren mit Online-Attacken recht häufig, Angriffsziele waren und sind hier z. B.:
    - Energiekonzerne, wie ENEL, General Electric, EDF und ENDESA,
    - Ölkonzerne, wie Exxon Mobil, Canadian Oil Sands und Imperial Oil,
    - Ölkonzerne unterstützende Banken wie The Royal Bank of Scotland,
    - Bergbauunternehmen in Guatemala und Peru,
    - Eisenbahnbaufirmen in Frankreich und der Schweiz, die Naturschutzgebiete zerstörten,
    - Bauunternehmen, die im Amazonasgebiet Staudämme errichten und damit Menschen und Natur gefährden.

Auch Sekten, Kriminelle, Spielseitenportale oder Rechtsradikale werden zu Zielen von hacktivistischen Aktionen. Die aufgeführten Beispiele sollen die Bandbreite an Zielobjekten veranschaulichen:

- 2011 meldete Anonymous, dass Mitglieder während einer Handzettelaktion in Mexiko von der kriminellen Vereinigung Los Zetas verschleppt worden seien. Anonymous drohte damit, die Identität von korrupten Journalisten, Polizisten und Taxifahrern offenzulegen, falls die entführten Anons nicht freigelassen werden (Operation Cartel). Widersprüchliche Nachrichten zum weiteren Verlauf kursierten im Internet, Anonymous meldete dann jedoch, die OpCartel sei erfolgreich verlaufen und die Mitglieder freigelassen.
- Verschiedene Hackerangriffe auf rechtsradikale Webseiten sind immer wieder Thema hacktivistischer Aktionen. So startete beispielsweise 2011 die Anonymous Operation Blitzkrieg, bei der Internetseiten rechtsextremen und -radikalen Ursprungs angegriffen wurden.
- Auch Internetnutzer, die kinderpornographische Inhalte konsumieren sowie Webseiten, die kinderpornographisches Material verbreiten, werden zum Ziel von

[97] Arns 2002, S. 65

Hacktivisten. Bespiele dafür sind das Vorgehen gegen einen kanadischen Pädophilen sowie die von Anonymous gestartete Operation SaveKids, die jeden Server zum Ziel erklären, der Kinderpornographie verbreitet.

- Die bereits beschriebene Aktion Chanology, die sich gegen die Sekte Scientology richtet, ist ein weiteres Beispiel für das breite Zielspektrum von Hacktivisten.

Die Ergebnisse der Fallanalyse zeigen, dass von 78 Geschädigten aus Deutschland 19 dem Bereich der Privatpersonen zuzuordnen sind, bei 16 handelt es sich um Schulen, bei 12 um Online-Versandhäuser und neun Geschädigte zählen zu dem Bereich Verein/Kirche. Verhältnismäßig wenig Geschädigte gehören zu dem wirtschaftlichen Bereich: Lediglich sieben Produktionsbetriebe und fünf Dienstleistungsunternehmen waren von hacktivistischen Angriffen betroffen und haben Anzeige erstattet (s. Abbildung 15). Dieses Ergebnis und die Tatsache, dass nur zwei Fälle von Hacktivismus gegen Behörden zu verzeichnen waren, entsprechen nicht den Erkenntnissen aus der Sekundäranalyse, in der festgestellt wurde, dass Hauptgeschädigte von Hacktivismus Regierungen, Polizei und Unternehmen sind. Hier muss jedoch berücksichtigt werden, dass es sich bei den Ergebnissen der Fallanalyse um die Wiedergabe des Hellfelds handelt und dieses insbesondere durch die Tatwahrnehmung und das Anzeigeverhalten der Geschädigten beeinflusst wird. Wie auch in anderen Kriminalitätsbereichen kann hier auf die These verwiesen werden, dass insbesondere Unternehmen aus Angst vor Imageverlusten (und weiteren Konsequenzen) im Bereich Cybercrime eher selten Anzeige erstatten und damit auch die Zahl geschädigter Unternehmen in der Fallanalyse vermutlich vergleichsweise niedrig ist.

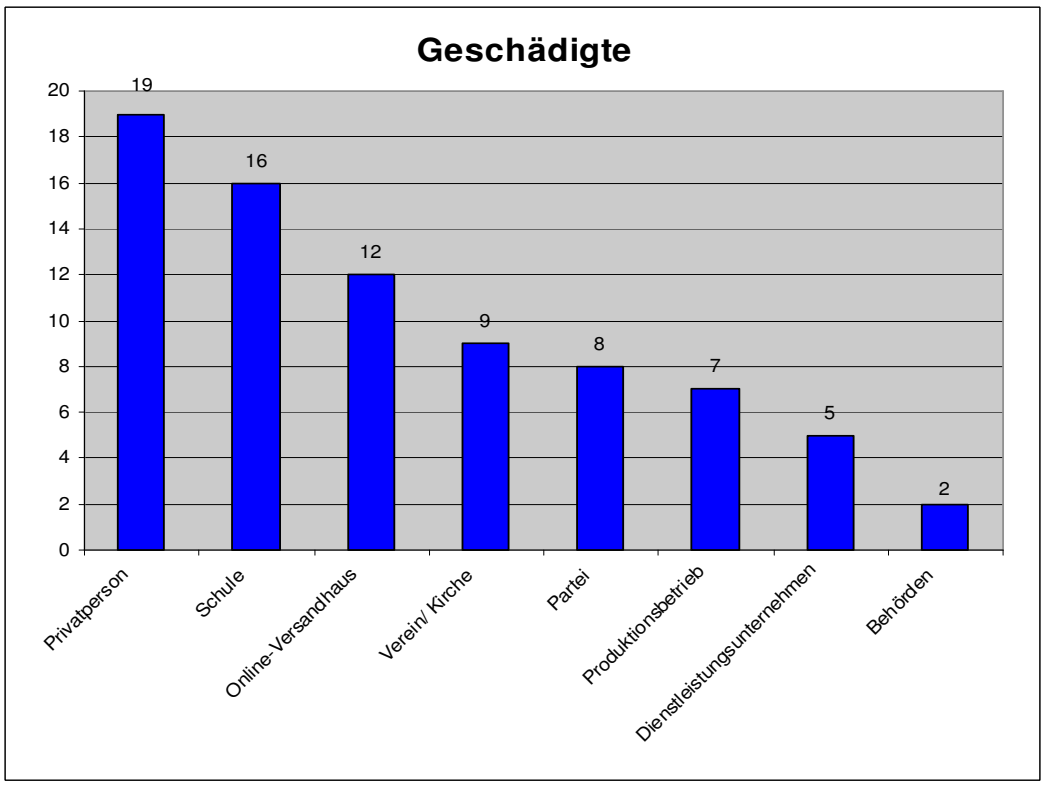


Abbildung 11: Geschädigte in 78 Fällen.

Die Schäden durch Hacktivismus können sowohl immaterieller als auch materieller Art sein. Trotz umfangreicher Literaturrecherchen ließen sich kaum gesicherte Aussagen zu finanziellen Schadenshöhen hacktivistischer Angriffe finden. Finanzielle Schäden können z. B. indirekt entstehen, wenn Versand- oder Dienstleistungs-Webseiten angegriffen wurden und Waren bzw. Dienstleistungen nicht bestellbar sind. Durch Imageschäden (die durch das öffentliche Bekanntwerden der Schädigung eintreten und damit häufig Grund für das Absehen von einer Anzeige sind) gehen Kunden und Aufträge verloren, der Umsatz sinkt und Aktienkurse fallen, wie dies z. B. im Fall eToy geschehen ist: Hier brach der Aktienkurs um 70 % ein und die Störung des vorweihnachtlichen Geschäfts führte aufgrund der Blockade zu schweren Einbußen.

Das Beheben der angerichteten Schäden kostet des Weiteren Zeit, Personal und Geld in unbestimmter Höhe.

Konkrete Zahlen nennt Verizon in seinem „2012 Data Breach Investigations Report“[98] zu gestohlenen und veröffentlichten Daten: Von 174 Millionen Angriffen, die mit der Veröffentlichung von Informationen in Verbindung stehen, werden - von Verizon gezählt- 58 % Hacktivisten zugeordnet. Damit stahlen Hacktivisten mehr Datensätze als kriminell motivierte Hacker. Bei einer Befragung deutscher Unternehmen stellte die Wirtschaftsprüfgesellschaft KPMG 2010 fest, dass ein Viertel der Firmen in den letzten drei Jahren von Cyberkriminalität betroffen waren.[99] Wie viele Hackerangriffe auf Hacktivisten zurückzuführen sind, ist jedoch nicht ersichtlich.

Sony gibt einen Schaden von fast 170 Millionen Dollar an, der durch den Angriff 2012 von Anonymous auf das PlayStation Netzwerk und der darauf folgenden Schließung des Spieleportals für über einen Monat entstand.
Medosch beziffert den Schaden infolge von DDoS-Attacken im Jahr 2000 auf CNN.com, Yahoo!, eBay und weiteren Servern auf 1,5 bis 3 Milliarden Dollar.[100]

Kaspersky Lab beziffert in einer Pressemitteilung vom 25.07.2013 den Schaden von gezielten Hackerangriffen auf Großunternehmen auf durchschnittlich 1,82 Millionen Euro pro Angriff. Davon werden 90 % zur Beseitigung der Schwachstellen, der Beschäftigung von externen IT-Experten und Anwälten sowie auf die Einschränkung der Geschäftsfähigkeit zurückgeführt. Die restlichen 10 % machen Investitionen in zukünftige präventive Maßnahmen aus. Kleinere und mittlere Unternehmen müssen, laut Kaspersky, mit einem Behebungsaufwand von ca. 70.000 Euro je Angriff rechnen.[101]

Mittels der durchgeführten Fallanalyse war es nicht möglich, ein genaueres Bild über die Höhe der finanziellen Schäden durch Hacktivismus zu zeichnen (s. Abbildung 16). Von 78 Fällen wurde in 61 Fällen keine Angabe dazu gemacht, ob ein Schaden entstand oder nicht. In zehn Fällen wurde ein (immaterieller) Schaden vermerkt, wobei dieser nicht quantifiziert

---

[98] Verizon (2013). *2013 Data Breach Investigation Report*. Im Internet: http://www.verizonenterprise.com/DBIR/2013/
[99] KPMG. (2010). *e-Crime-Studie 2010. Computerkirminalität in der deutschen Wirtschaft*. Im Internet: https://www.kpmg.de/docs/20100810_kpmg_e-crime.pdf
[100] Medosch, A. (2001). *The Kids are out to play*. In: A. Medosch/J. Röttgers. (Hrsg.): *Netzpiraten. Die Kultur des elektronischen Verbrechens*. Verlag Heinz Heise. Hannover. S. 117-127
[101] Kaspersky. (2013). *Millionenschäden durch gezielte Cyberangriffe auf Großunternehmen*. Pressemitteilung vom 25.07.2013. Im Internet: http://newsroom.kaspersky.eu/fileadmin/user_upload/de/Downloads/PressReleases/074_PM_B2B_Targeted_Attacks_final.pdf

werden konnte. In drei Fällen lag der monetäre Schaden unter 100 Euro, in zwei Fällen bewegte sich der Schaden zwischen 101 und 10.000 Euro und in zwei Fällen lag der Schaden über 10.000 Euro (12.000 und 150.000 €).

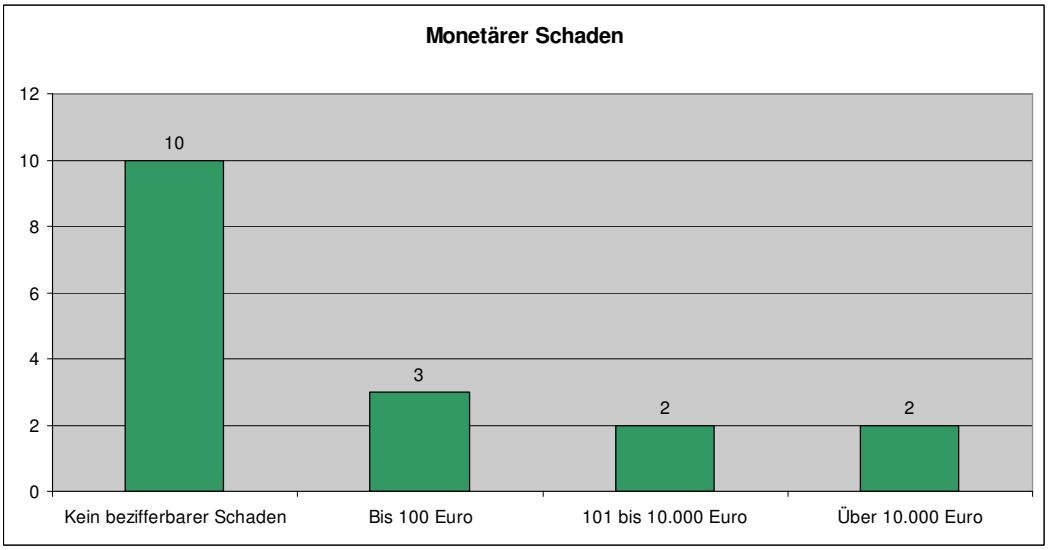


Abbildung 12: Schaden in 17 Fällen; 61 Fälle ohne Angaben.

4.2.5 Einzeltäter oder Gruppierungen

Valide Aussagen zu Merkmalen hacktivistischer Täter zu machen, ist, wie bei anderen Cybercrime-Tätertypen auch, generell schwierig. Die Täter agieren anonym und häufig unbemerkt. In Foren geben Hacktivisten nur wenig von sich preis und wenn sie dies tun, dann ist die Richtigkeit dieser Angaben nicht garantiert.

Da sich soziales und politisches Engagement überwiegend in Gruppen ausdrückt, weiß man auch von mehr hacktivistischen Gruppierungen als von Einzeltätern.[102] Ob es sich bei Angriffen um die Taten von hacktivistischen Einzeltätern oder Gruppierungen handelt, lässt sich oft an mitgelieferten (oder später kommunizierten) Bekennungen zur Tat festmachen.

Die Ergebnisse der Fallanalyse zeigen, dass es in 43 Fällen (55,1 %) eine Täterbekennung gab. In 20 Fällen (25,6 %) gab es keine Bekennung und in 15 Fällen (19,2 %) wurde hierzu in den analysierten Akten keine Angabe gemacht (s. Abbildung 17).

[102] Hampson 2012

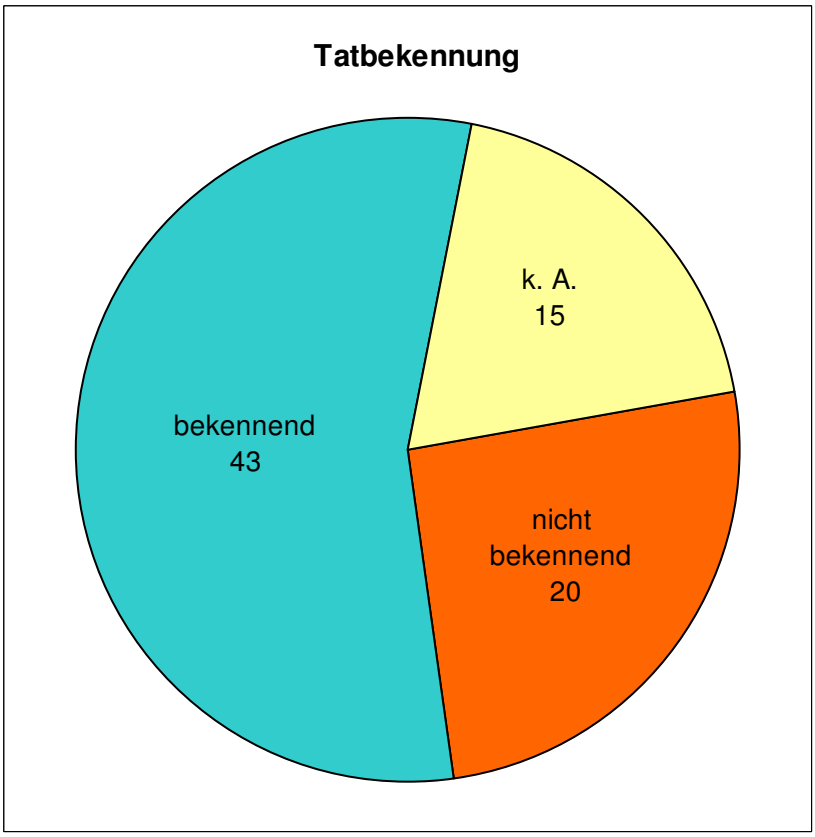


Abbildung 13: Vom Täter hinterlassene Bekennung zur Tat.

Wie bereits in Kapitel 4.2.3 dargestellt, gibt es eine Vielzahl bekannter und (mehr oder weniger) aktiver Hacktivistengruppen:

- Anonymous,
- Cult of the Dead Cow (cDc),
- The Electronic Disturbance Theater (EDT),
- Die ElectroHippies,
- Hacktivistengruppe World´s Fantabulous Defacers (WFD),
- Kaotik Team,
- sp10it,
- Asthray Lumberjacks,
- Wannabe Hacker,
- Telecomix,
- 4ATA (Fourth Awaking People´s Army)
- weitere Gruppen.

In der Fallanalyse handelte es sich in 30 Fällen um Bekennungen, die eindeutig einer Gruppierung zugeordnet werden konnten (s. Abbildung 18). Die restlichen 13 Bekennungen (s. o.) ließen weder eine dahinterstehende Gruppierung noch einen Einzeltäter erkennen. Auch gab es – trotz Bekennungen – in den Ergebnissen keine eindeutigen Hinweise auf Einzeltäter. Dagegen ließen sich 15 hacktivistische Gruppierungen mit Namen ausmachen:

Fälle nach Gruppenzugehörigkeit			
1923 Turk Group	2	NMTD TIM	1
Anonymous	11	No Name Crew	1
AYYILDIZ TEAM	5	Pisagor - Soldiers of Allah	1
Dark Mare Crew	1	PKK	1
F.A.T. Federal Attack Team	1	Team Sality	1
Group Hp-Hack	1	Turkish Republican Hackers	1
Group x3	1	Underground Nazi Hacktivist Group	1
Misfits CST	1		

Abbildung 14: Hacktivistische Gruppierungen mit Fallzahl.

Von den wenigen bekannten Einzeltätern agieren einige zwar allein, aber dennoch mit Sympathien zu bestimmten Hacktivistengruppen.[103]

Im Frühjahr 1998 erlangte ein junger britischer Hacker, der sich JF nannte, Zugang zu ca. 300 Webseiten, auf denen er Antinuklear-Botschaften und -Bilder postete. ‚Milw0rm' brach in das Computersystem des indischen Bhabha Atom Forschungscenter, Bombay ein, ebenfalls um gegen nukleare Waffentests zu protestieren.

Der damals 15-jährige Norweger Jon Johansen entwickelte 1999 eine Software (DeCSS) mit deren Hilfe verschlüsselte DVDs auch auf dem Linux System abspielbar wurden und stellte sie ins Internet. Ein Nebeneffekt war, dass somit auch der Kopierschutz der DVDs aufgehoben wurde. Samuel stellt in ihrer Arbeit den Fall als Hacktivismus vor, da die Intention des Hacks von Johansen auf die politische Forderung nach Informationsfreiheit beruhte.[104]

Der Hacker Jester (th3j35t3r) bezeichnet sich selbst als „Hacktivist der guten Seite"[105]. Er legte WikiLeaks lahm, entwickelte eigene Hackerprogramme, wie das DoS-Tool XerXes, und griff islamistische Seiten an. Im November 2010 brachte Jester mit einer DoS-Attacke gegen WikiLeaks.org die Seite für 24 Stunden zum Zusammenbruch. Er begründete sein Vorgehen

[103] Jordan 2001
Jordan/Taylor 2004
[104] Samuel 2004
[105] Paget 2012, S. 8

damit, dass mit der Veröffentlichung von 250.000 von der US-Regierung gestohlenen Dokumenten das Leben „*unserer Truppen*“[106] aufs Spiel gesetzt worden sei.
Ein Hacker in der Türkei manipulierte im Januar 2010 ein Computersystem, mit dem Gläubige zum Gebet gerufen werden und ersetzte die ursprünglichen Nachrichten durch den Text eines Künstlers, der bekannt ist für seinen Kampf für Anerkennung von Homosexualität in der Türkei.[107]
Im April 2010 rief ein Professor der Universität San Diego zu einem DDoS-Angriff auf Universitäts-Webseiten auf, um bessere Chancen für benachteiligte Studenten durchzusetzen.[108]

4.2.6 Soziodemographische und -ökonomische Tätermerkmale

Es gibt nur wenige Studien, die das Alter von Hacktivisten angeben. Aus verschiedenen Quellen lässt sich 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.[109]
Das Durchschnittsalter der von Rheinberg und Tramp (2006) untersuchten Probanden, die sich intensiv mit Computern beschäftigen, lag bei knapp 25 Jahren.[110]

Von den 37 Beschuldigten, die in der Fallanalyse genauer untersucht wurden, war auch hier, ähnlich zu der Altersverteilung der festgenommenen Anonymous-Mitglieder, die Mehrheit zwischen 14 und 28 Jahre alt. Acht Beschuldigte waren über 28 Jahre alt (s. Abbildung 19).

[106] Hampson 2012, S. 512
[107] Paget 2012
[108] ebd.
[109] Kelly 2012
[110] Rheinberg, F./Tramp, N. (2006). *Anreizanalyse intensiver Freizeitnutzung von Computern: Hacker, Cracker und zweckorientierte Nutzer*. In: Zeitschrift für Psychologie. 214. 97-107

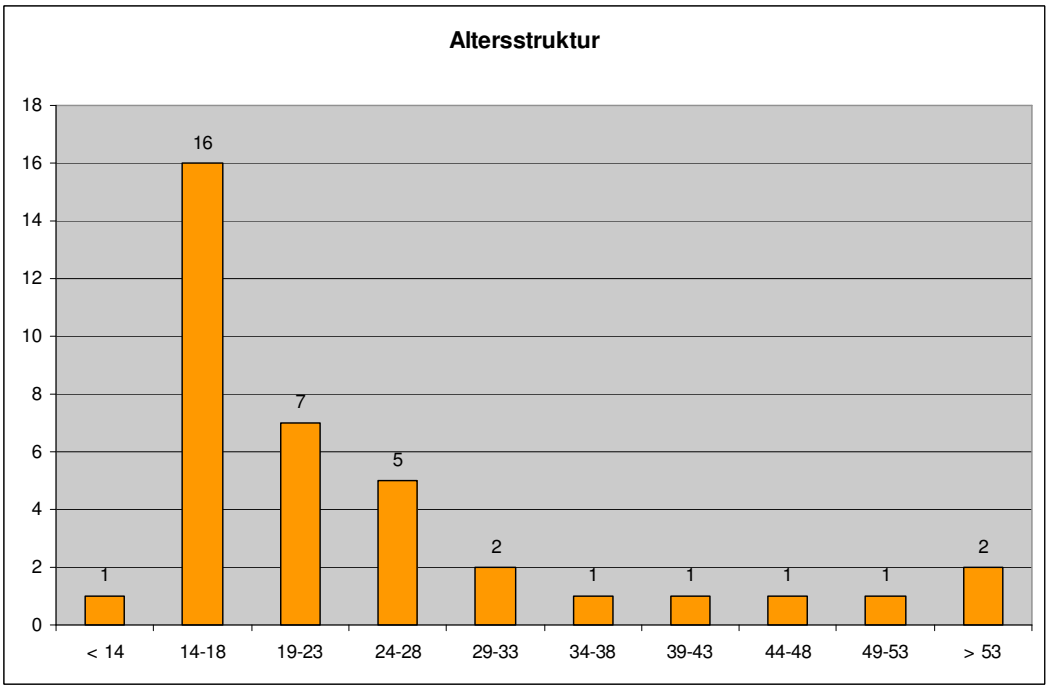


Abbildung 15: Altersverteilung bei 37 Beschuldigten.

Wissenschaftlich fundierte Aussagen zum Geschlecht von Hacktivisten sind ebenfalls kaum zu finden. Verschiedene Studien gehen von einem geringen Anteil weiblicher Hacktivisten aus. So ist der überwiegende Anteil von Probanden der Studie von Rheinberg und Tramp, die sich mit intensiven Computernutzern – nicht nur mit Hackern – beschäftigte, männlich (86,6 %).[111] Auch Kelly schließt aufgrund des durchgehend männlichen Geschlechts von verhafteten Hackern auf einen stark unterrepräsentierten weiblichen Anteil in der Hacktivistenszene.[112] Jordan und Taylor vermuten die Ursache dieser Unterrepräsentation weiblicher Hacker zum einen in den sozialen Konditionen der IT-Branche, die es Frauen erschweren, in programmierenden Tätigkeiten Fuß zu fassen, zum anderen in der Natur des kriminellen Hackens, die mit Zerstören und Randalieren einhergeht und damit weniger zu weiblichen Eigenschaften passen würde.[113]

Die Fallanalyse kam zu folgendem Ergebnis: 76 % der 37 Beschuldigten sind männlich und immerhin 24 % weiblich (s. Abbildung 20). Auch wenn dieses Ergebnis auf den ersten Blick einem stark unterrepräsentierten weiblichen Anteil in der Hacktivistenszene (s. o.) widerspricht, so müssen die Selektionseffekte berücksichtigt werden: lediglich ein Verfahren

[111] Rheinberg, F./Tramp, N. (2006).
[112] Kelly 2012
[113] Jordan/Taylor 2004

mit 37 Beschuldigten bot Informationen zu soziodemographischen und -ökonomischen Tätermerkmalen.

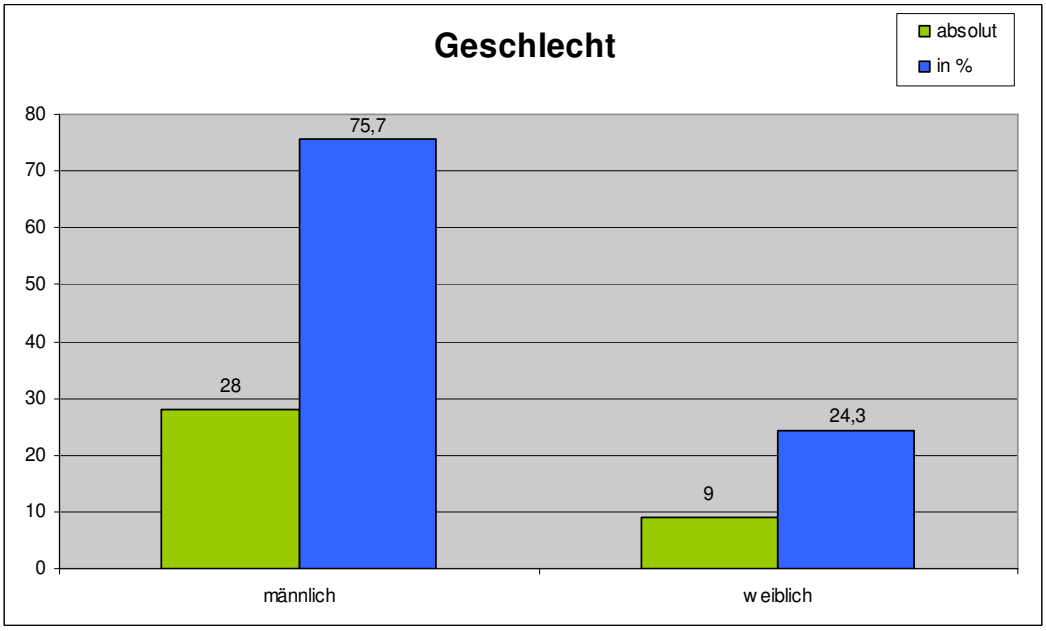


Abbildung 16: Geschlechterverteilung bei 37 Beschuldigten.

In der Fallanalyse wurde auch die Staatsangehörigkeit der Beschuldigten erhoben, mit einem eindeutigen Bild: Die Mehrheit (28 Personen) ist im Besitz der deutschen Staatsangehörigkeit. Vier Beschuldigte sind türkische Staatsangehörige und ein Beschuldigter hat die kroatische Staatsangehörigkeit. Zu vier Beschuldigten fehlten entsprechende Angaben (s. Abbildung 21).

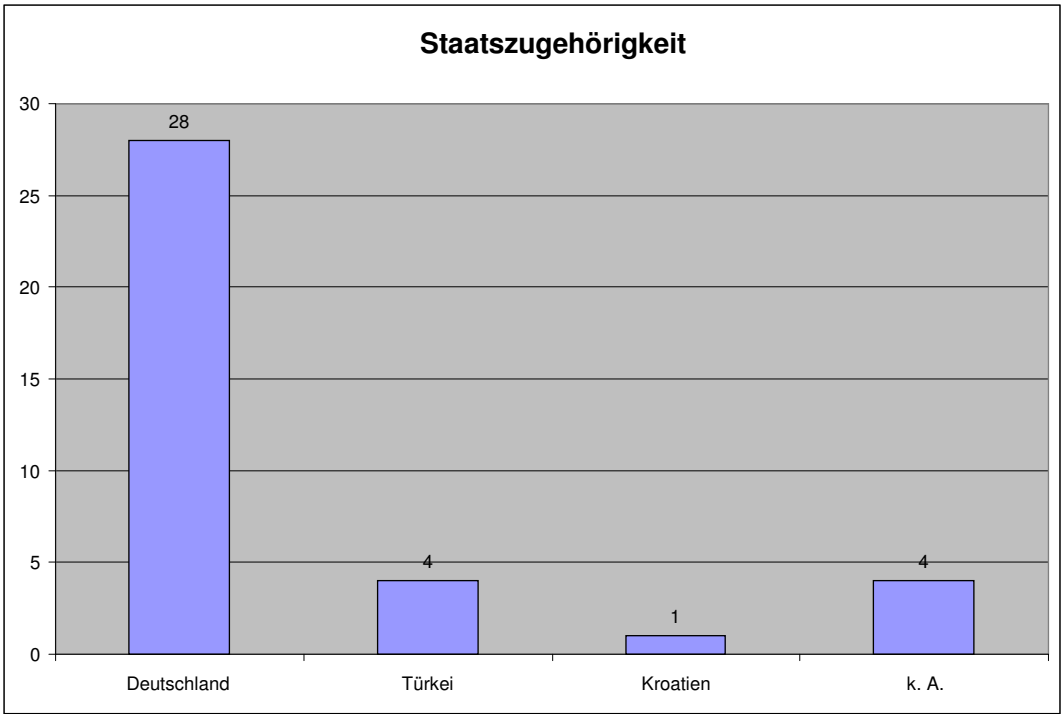


Abbildung 17: Staatszugehörigkeit bei 37 Beschuldigten.

Zum Zeitpunkt der Durchführung der Sekundäranalyse lagen keine einschlägigen Untersuchungen zu sozioökonomischen Merkmalen von Hacktivisten vor. So ist bislang weder bekannt aus welchem sozialen Umfeld Hacktivisten vornehmlich stammen, noch welchem Bildungsstand oder welchen Berufsgruppen sie angehören.

In der Fallanalyse wurden die sozioökonomischen Merkmale Bildung und Beschäftigungsstatus erhoben. Darüber hinaus lieferte das Material keine weiteren sozioökonomischen Merkmale. Im Bereich Bildung wurden in 27 Fällen überhaupt keine Angaben gemacht. Acht Beschuldigte hatten einen Realschulabschluss, einer verfügte über Abitur und einer besaß den Hauptschulabschluss (s. Abbildung 22). Lässt man die mangelnde Repräsentativität dieser Ergebnisse außen vor, könnte man daraus schließen, dass die Mehrzahl hacktivistischer Taten von Beschuldigten der mittleren Bildungsschicht begangen wird.

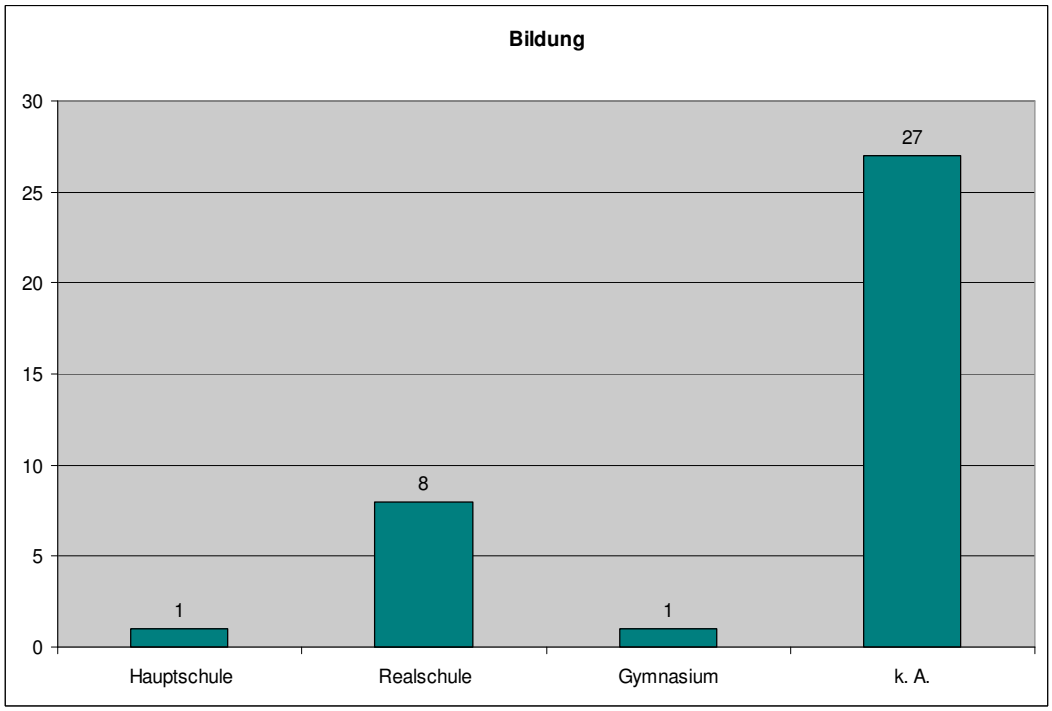


Abbildung 18 Bildungsstatus bei 37 Beschuldigten.

Zum Beschäftigungsverhältnis wurde in 19 Fällen festgestellt, dass es sich bei den Beschuldigten um Schüler, Studenten oder Auszubildende handelte, was im Zusammenhang mit der Altersverteilung erwartbar war. Vier Beschuldigte waren arbeitslos und einer angestellt. In 13 Fällen wurde in den Akten keine Angabe zum Beschäftigungsverhältnis gemacht (s. Abbildung 23).

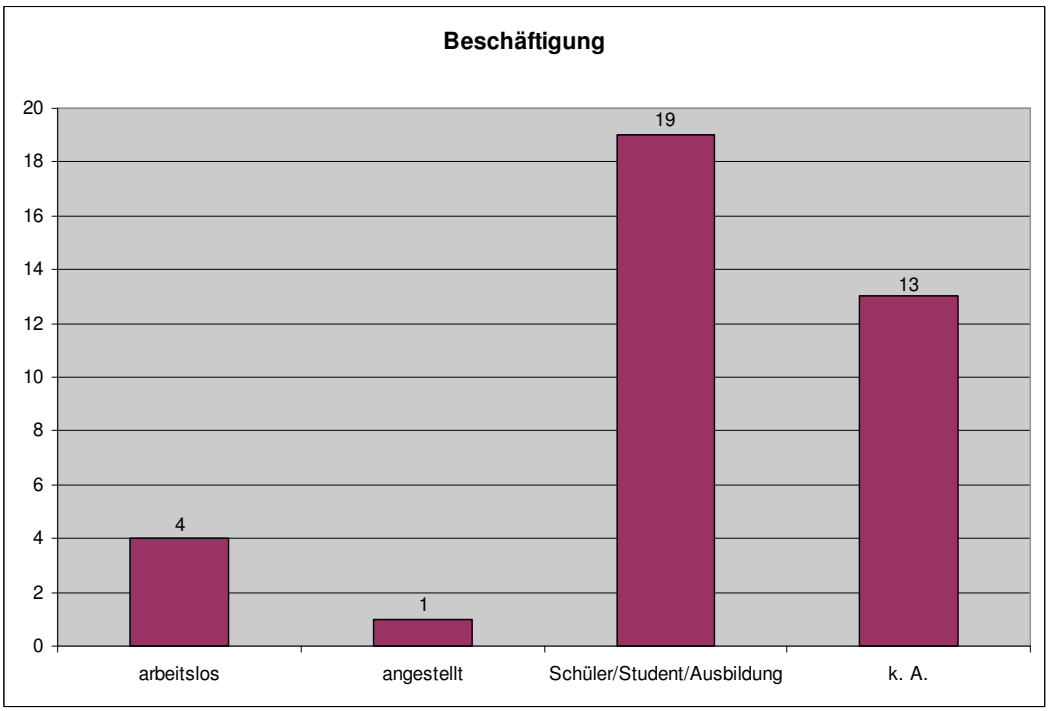


Abbildung 19: Beschäftigungsstatus bei 37 Beschuldigten.

4.2.7 Motive und Zielrichtungen

Da es sich beim Hacktivismus inhaltlich um die Schnittmenge der Konzepte Hacking und Aktivismus handelt bzw. um aktivistische Ziele, die mittels Hacking-Tools/-Optionen umgesetzt werden, sollte dies auch für die Motive der Hacktivisten gelten. Neben den ideologischen Motiven aus dem aktivistischen Bereich, die sich in den Aktionen selbst widerspiegeln, können für den einzelnen Hacktivisten weitere emotionale Motivationen eine Rolle spielen, von denen sich einige auch bei Hackern finden.

Es gibt nur wenige Forschungsergebnisse zu den persönlichen Motiven von Hacktivisten, was an der durch die Anonymität im Cyberraum bedingten Schwierigkeit liegt, hacktivistisch Agierende gezielt zu erreichen.

Die Möglichkeit, die Motivation einer Person aus den Zielen zu erschließen, ist nicht ausreichend valide, da eine Aktion im Kontext politischer Überzeugungen sich nicht unbedingt von einer Aktion aus reinen Spaßmotiven unterscheiden muss, wenn entsprechende Bekennungen zur Zielrichtung und Zweck fehlen.

Es ist jedoch möglich, Rückschlüsse aus Studien zu der Motivlage von Hackern zu ziehen, da diese in einigen Punkten mit der persönlichen Motivlage von Hacktivisten übereinstimmen dürfte (s. o.).

Einzelne befragte Hacker äußerten das Motiv Spaß (= just for the lulz): So führt die Angabe „*just for the lulz*“ bei der von zone-h geführten Statistik über die Motivationen von Hackern, warum sie Seiten defacen, die Liste weit vor anderen genannten Gründen an.[114]

Bachmann (2010) untersuchte Motive und Eigenschaften von 124 Hackern mittels einer Fragebogenstudie. Im Ergebnis unterscheiden sich Hacker vom durchschnittlichen Computer-/Internetnutzer einerseits durch ein höheres Risikoverhalten und andererseits durch eine rationellere Denkweise. Hacker bevorzugen schwere, komplexe Aufgaben und genießen es, Lösungen dafür zu finden.[115]
Diese Ergebnisse stimmen auch mit denen von Rheinberg und Tramp (2006) überein, die Anreizdimensionen intensiver Computernutzer für verschiedene Aktivitäten untersuchten.[116]
Beiden Studien ist zu entnehmen, dass ein Hauptmotiv von Hackern das sogenannte *Sensation Seeking* ist, also das Suchen nach abwechslungsreichen, neuen und komplexen Eindrücken und Erlebnissen im Cyberraum bzw. mittels Nutzung von Informations- und Kommunikationstechnologien.
Sensation Seeking kann auch dem Motiv entspringen, Langeweile durch Spannungserzeugung zu bekämpfen. Der Hacker Maelstrom äußerte sich folgendermaßen:

> „*[…] the adrenaline rush I get when I'm trying to evade authority, the thrill I get from having written a program that does something that was supposed to be impossible to do […].*“[117]

Das Gefühl der Macht und Kontrolle über andere wie z. B. über Konzerne und Regierungen zu haben, wird von Hackern ebenfalls als Motivation genannt.

Viele der Vorgehensweisen im Bereich Hacktivismus, wie z. B. DDoS-Angriffe, erfordern die Zusammenarbeit mehrerer Akteure und fördern das Zusammengehörigkeitsgefühl und die Gruppenidentität, zwei Effekte, die sich auch positiv auf den Einzelnen auswirken.[118] Auch in den Ergebnissen der Untersuchung von Rheinberg und Tramp (2006) wird der Gruppenzugehörigkeit ein hohes Anreizpotential für diverse Aktivitäten intensiver

[114] http://www.zoneh.org
[115] Bachmann, M. (2001). *The Risk Propensity and Rationality of Computer Hackers*. In: International Journal of Cyber Criminology. Vol. 4, (1&2). S. 643-656
[116] Rheinberg, F./Tramp, N. (2006).
[117] Jordan/Taylor 2004, S. 128
[118] Samuel 2004

Computernutzer zugemessen, was gegen das Stereotyp des vor dem Computer sitzenden, „*kontaktgestörten Einsiedler*[s]“[119] spricht.

Ein wichtiger Motivationsfaktor für Hacker ist die Anerkennung und der Respekt der Hacking-Gemeinschaft. Dieser Teil der Mischung aus Motivlagen von Hackern und Aktivisten (s. o.) spiegelt sich auch in Aussagen von Hacktivisten wider: So sagt beispielsweise Ca$h Money, ein Mitglied der Hacktivistengruppe Hacktivismo: „[…] *everyone´s respected for what you do* […]“.[120]

Die ideologischen Ziele von Hacktivisten unterscheiden sich oftmals von Gruppierung zu Gruppierung. Überwiegend häufig ist in fast allen Gruppen jedoch die Forderung nach einem freien, unzensierten und jedermann zugänglichem Internet vertreten.
Daneben führen die Gruppierungen unterschiedliche Aktionen z. B. gegen Rassismus, Nationalsozialisten, Scientology, Pädophile, Strafverfolgungsorgane, Regierungen, Organisationen oder gegen (vermeintlich) korrupte Firmen durch.
Für Aktionen von Anonymous konnten Stimmen der Teilnehmer festgehalten werden, die im Folgenden beispielhaft die ideologischen Ziele der Gruppen (und des einzelnen) wiedergeben:

> „*Das Ziel ist einfach: Gewinne das Recht, das Internet frei von jeglicher Kontrolle durch irgendeine Macht, Firma oder Regierung zu halten*.“[121]
>
> „*Ich kämpfe mit AnonOps, weil ich glaube, dass das gegenwärtige System fehlschlug und dass ein System, das auf Anarchie basiert, das einzig brauchbare ist*.“[122]
>
> „*Wir sind gegen Firmen und Regierungen, die das Internet behindern. Wir glauben, dass es für jeden frei und offen sein sollte. Regierungen sollten nicht versuchen es zu zensieren, wenn sie mit Inhalten nicht einverstanden sind* […].“[123]
>
> „*Wir unterstützen WikiLeaks nicht, weil wir für oder gegen die Inhalte sind, die veröffentlicht wurden, sondern weil wir gegen Zensur im Internet sind*.“[124]
>
> „*Die Hauptmotivation* [bei der Operation Megaupload] *ist nicht die Verteidigung von Megaupload, sondern der Kampf gegen Internetzensur*.“[125]

[119] Rheinberg, F./Tramp, N. (2006). S. 14
[120] Samuel 2004, S. 131
[121] Fitri 2011, S. 9
[122] McLaughlin 2012, S. 65
[123] Fitri 2011, S. 10
[124] ebd.

In der Fallanalyse wurde das vorliegende Material auf Merkmale zur Motivlage und zum politischen Hintergrund untersucht. Die Motivlage war entweder bereits vom entsprechenden Sachbearbeiter bei der Fallbearbeitung in den Akten vermerkt worden oder wurde durch das Projektteam anhand von Bekennungen oder speziellen Auffälligkeiten des Falls hinzugefügt. Im letzteren Fall handelte es sich z. B. um Web-Defacements, die keinen Zusammenhang von Verursachern und Geschädigten erkennen ließen. Hier besteht die Vermutung, dass es sich um automatisierte Web-Defacements handelt, die zu Übungszwecken Webseiten automatisch nach Sicherheitslücken abtasten, um sich dann ggf. auf entsprechenden Seiten zu platzieren. Zehn Fälle entsprachen einer solchen Auffälligkeit und wurden dem Motiv „Übung“ zugeordnet. Acht Fälle entsprachen dem Motiv der Wettbewerbsverhinderung. Das bedeutet, dass Webseiten gezielt manipuliert wurden, um Konkurrenten (in verschiedenen Vorgängen) auszuschalten. Ein auf zone-h geposteter Fall diente offensichtlich nur der Prahlerei. Die restlichen Fälle wurden den klassischen aktivistischen Motiven Propaganda (22 Fälle) und Protest (32 Fälle) zugeordnet (s. Abbildung 24).

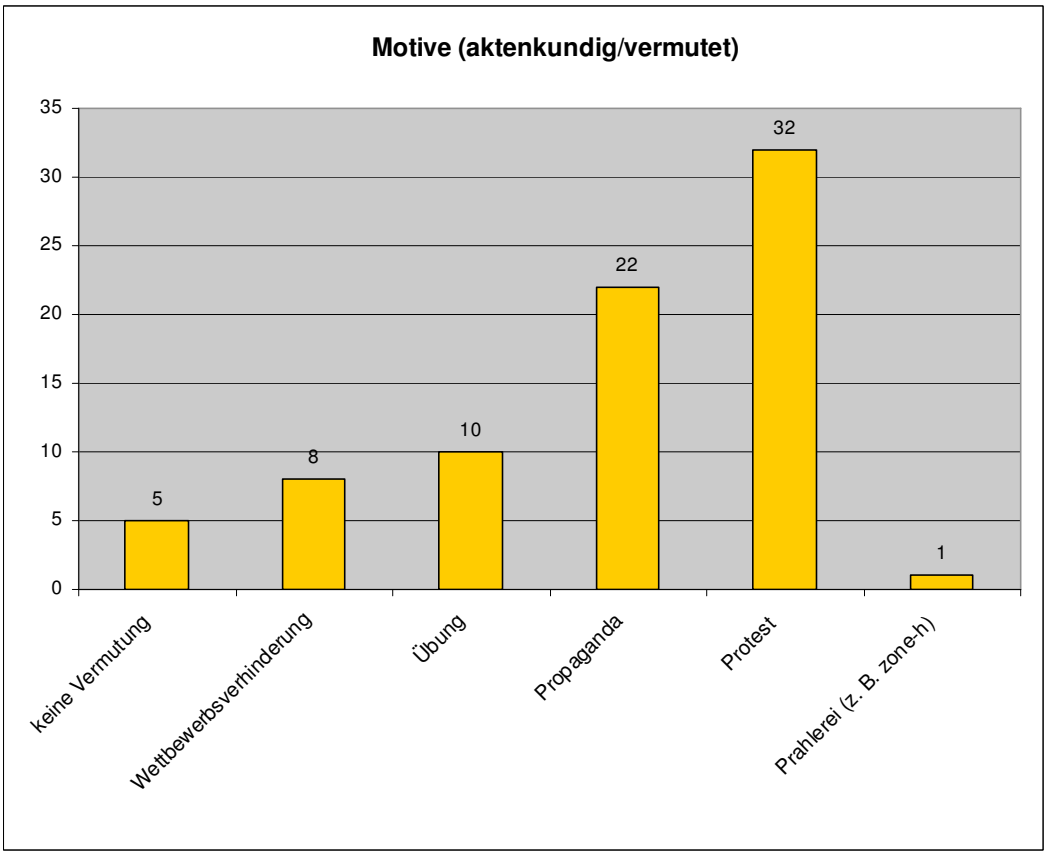


Abbildung 20: Motivlage in 78 Fällen.

[125] Paget 2012, S. 20

Der politische Hintergrund der Taten aus der Fallanalyse ließ sich überwiegend der Politisch Motivierten Kriminalität (PMK) links zuordnen (24 Fälle), wohingegen nur vier Fälle aus dem Bereich der PMK rechts kamen. 20 Fälle stammten aus dem allgemeinen PMK Bereich (hierzu gehört auch die PKK). Ein islamistischer Hintergrund ließ sich in sieben Fällen erkennen, in 23 Fällen konnte der politische Hintergrund nicht eindeutig zugeordnet werden (s. Abbildung 25).

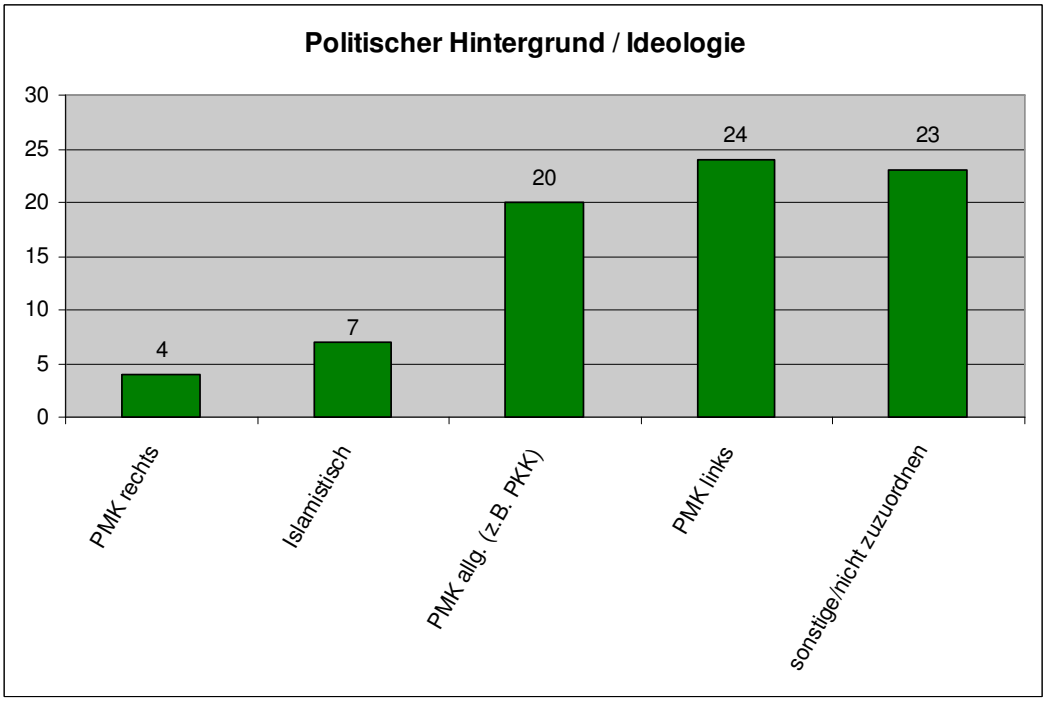


Abbildung 21: Politischer Tathintergrund in 78 Fällen.

4.3 Zusammenfassung und Zusammenhänge

Das begriffliche Phänomen „Hacktivismus“ tauchte erstmals in den 90er Jahren im Zusammenhang mit der Gruppe Cult of the Dead Cow (cDc) auf, die als eine der ersten hacktivistischen Gruppierungen gilt. Am Anfang ging es Hacktivisten insbesondere um den Protest gegen Zensur im Internet. Es wurde der freie Fluss von Informationen gefordert. Gruppierungen wie The Electronic Disturbance Theater (EDT) ElectroHippies, World´s Fantabulous Defacers (WFD), Team sp10it, Asthray Lumberjacks, die Wannabe Hacker und weitere Hacktivistengruppen setzten sich neben einem freien Internet auch zunehmend für soziale Zwecke und Rechte ein und protestierten mittels Hackerangriffen und -tools gegen politische sowie wirtschaftliche Ereignisse und Regularien. Insbesondere Anonymous macht(e) immer wieder auch medial auf sich aufmerksam: Der Öffentlichkeit präsentieren sich die Mitglieder

mit einer Guy-Fawkes-Maske, ihr Slogan „*Anonymous is Legion. We do not Forgive. We do not Forget. Expect us.*“ begleitet digitale Protestschreiben, Bekennungen und Aufrufe zur Teilnahme. Anonymous führt immer wieder (einmalige sowie fortlaufende) „Operationen“ genannte hacktivistische Aktionen durch. Aus Anonymous formierten sich hacktivistische Ablegergruppierungen wie LulzSec, AntiSec und MalSec, die ähnliche Aktionen wie Anonymous durchführen und zum Teil auch aus denselben Sympathisanten bestehen.

Über (Chat-)Foren, IRC, Twitter, Facebook usw. werden hacktivistische Aktionen geplant und Sympathisanten für die Organisation und Durchführung von Aktionen mobilisiert. Die Vorgehensweise in vielen Aktionen ist das Ausführen verschiedener Angriffstechniken, die nicht exklusiv auf das Phänomen Hacktivismus beschränkt sind, sondern auch Anwendung in anderen Cybercrime-Bereichen finden. Neben den verschiedenen Angriffstechniken zählen zu der Vorgehensweise auch Ausspäh- und Verschleierungstechniken zur Anonymisierung des Angreifers. Von Hacktivisten häufig gewählte Vorgehensweisen sind Web-Defacements, das Eindringen in fremde Server und die Manipulation von Daten. Auch DDoS-Angriffe werden als Protestmittel eingesetzt. Anhand der Erkenntnisse aus Studien scheint diese Form jedoch von Hacktivisten weniger häufig genutzt zu werden. Dies kann jedoch auch ein Ergebnis von Selektionseffekten sein, so dass im Dunkelfeld weitaus mehr DDoS-Angriffe auftreten.

Angriffsziele von Hacktivisten sind laut Sekundäranalyse in erster Linie Regierungen und staatliche Organe, wie z. B. Polizeien und Sicherheitsbehörden. Daneben geraten auch Firmen, Banken und Konzerne immer wieder in den Fokus von Hacktivisten. Vermutlich (auch) dem Anzeigeverhalten von Unternehmen geschuldet, tauchen in den Ergebnissen der Fallanalyse überwiegend Privatpersonen, Schulen und Online-Versandhäuser auf. Angaben zu Schäden werden kaum erfasst, häufig lassen sich über die Höhe finanzieller Schäden nur Vermutungen anstellen. Die aus der Fallanalyse gewonnenen Zahlen bewegen sich hier – je nach Zielobjekt und Vorgehensweise – zwischen 0 und 150.000 Euro pro Fall.

Die Ergebnisse der Fallanalyse wurden für wesentliche Merkmale in Kreuztabellen ausgewertet, um ggf. unbekannte Zusammenhänge entdecken zu können.
Betrachtet man die Geschädigten nach jeweils eingesetzten modi operandi, so fällt lediglich auf, dass Web-Defacements für den Angriff auf alle Kategorien von Geschädigten gleichermaßen eingesetzt wurden. Das Ausspähen von Daten wurde überwiegend von Privatpersonen zur Anzeige gebracht (s. Abbildung 26).

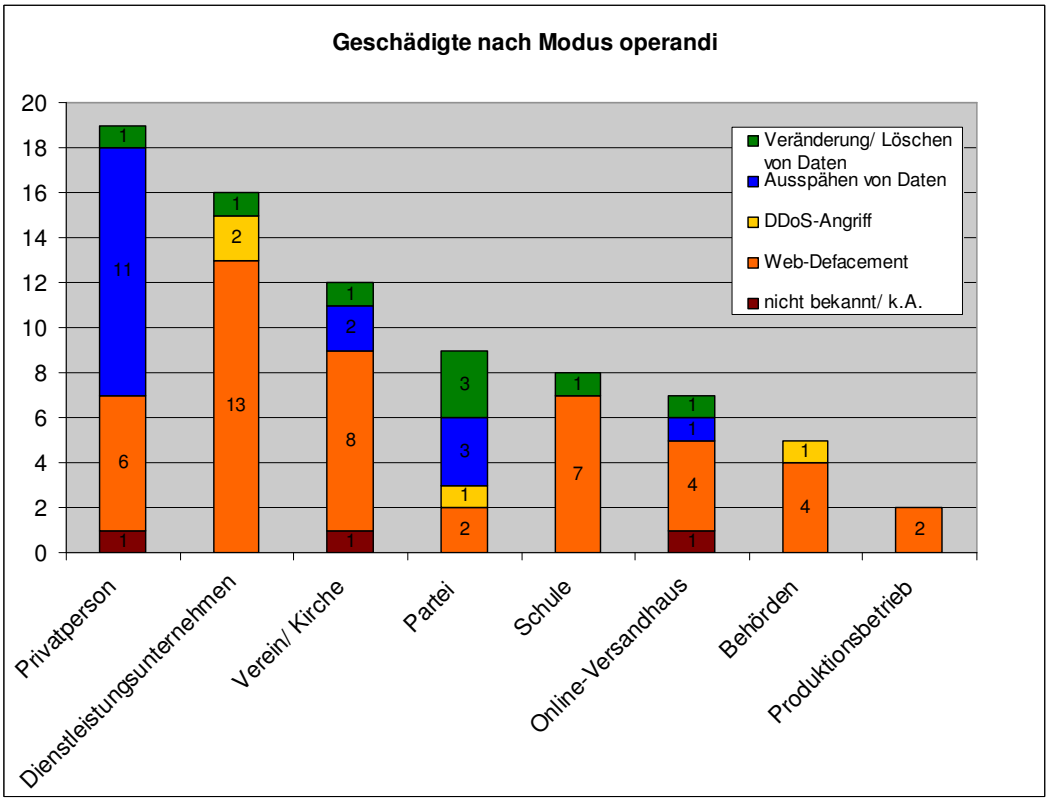


Abbildung 22: Vorgehensweise bezogen auf Geschädigte in 78 Fällen.

Es lässt sich darüber hinaus nicht feststellen, dass bestimmte modi operandi für gewisse Schadenshöhen verantwortlich sind (s. Abbildung 27). Schadenssummen über 10.000 Euro lassen sich sowohl für das Ändern/Löschen von Daten als auch DDoS-Angriffe und Web-Defacements ausmachen. Da jedoch lediglich in 17 Fällen Angaben zum Schaden gemacht wurden und sich Aussagen zur Schadenshöhe in nur sieben Fällen finden lassen, sind diese Ergebnisse nicht valide interpretierbar.

Dies gilt auch für die Interpretation der Aufschlüsselung der Schadenshöhe bezogen auf den Geschädigten, auch wenn sich hier zeigt, dass insbesondere Dienstleistungsunternehmen Angaben zur Schadenshöhe gemacht haben (s. Abbildung 28).

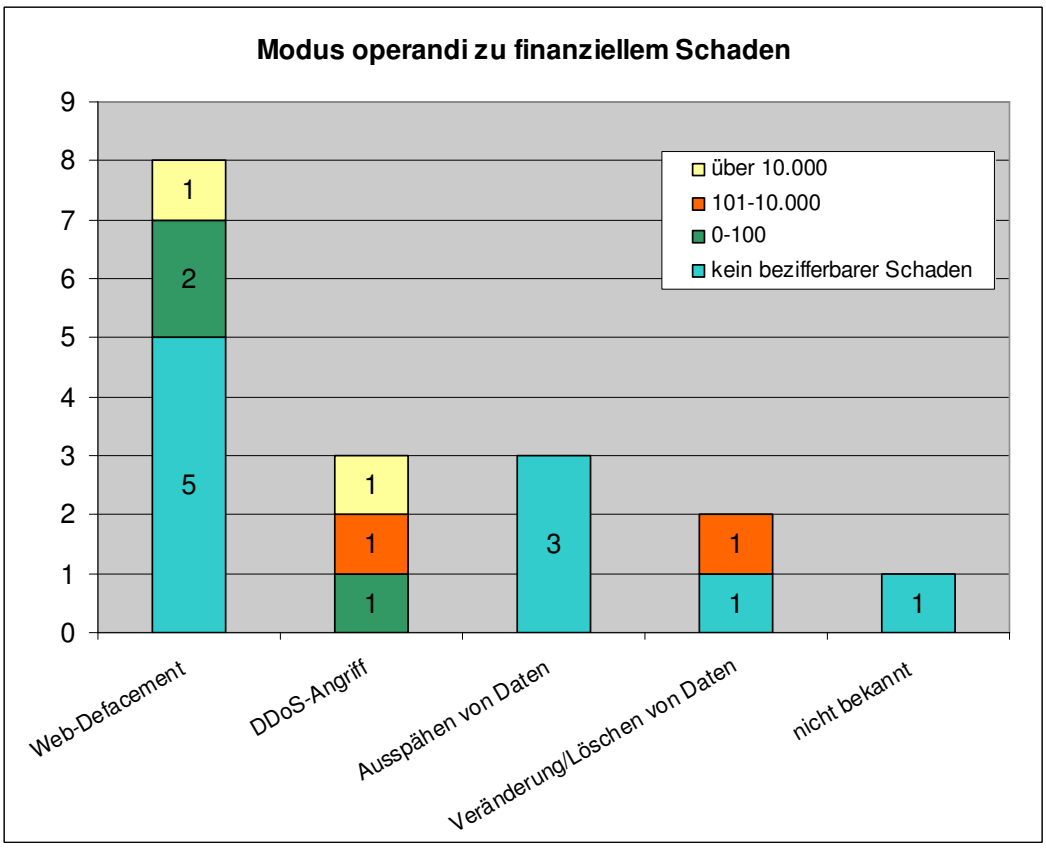


Abbildung 23: Schaden nach Vorgehensweise in 17 Fällen; 61 Fälle ohne Angaben.

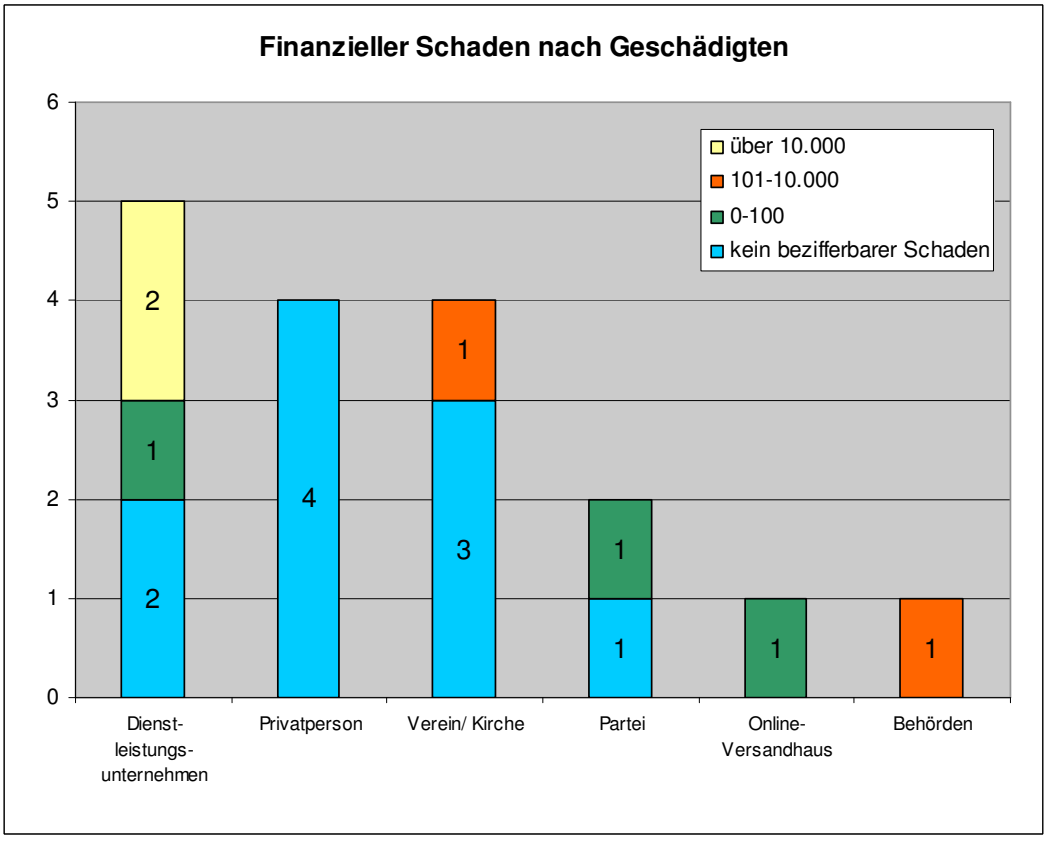


Abbildung 24: Schaden bezogen auf Geschädigte in 17 Fällen; 61 Fälle ohne Angaben.

Grundsätzlich lassen sich für die vorgestellten Merkmale mittels kreuztabellarischer Auswertung keine signifikanten Auffälligkeiten und Zusammenhänge erkennen.

Politisches Engagement wird überwiegend in Gruppen ausgedrückt und auch Hacktivisten agieren häufig in Gruppierungen. Daneben gab es in der Vergangenheit immer wieder auch Aktionen, zu denen sich einzelne Hacktivisten bekannten. Viele hacktivistische Taten lassen sich nicht eindeutig einer Gruppierung zuordnen oder überhaupt nach Einzeltäter oder Gruppentat differenzieren, insbesondere wenn entsprechende Hinweise, wie z. B. Bekennungsschreiben zur Tat oder entsprechend signierte Web-Defacements, fehlen.

In der Fallanalyse wurde auch untersucht, bei welchen modi operandi am ehesten eine Bekennung vom Täter „mitgeliefert“ wurde. Hier sticht mit 34 Fällen ganz klar das Web-Defacement hervor, da hier entsprechende Signaturen und Bekennungen bereits im Defacement platziert wurden. Aber auch in drei Fällen von DDoS-Angriffen und sechs Fällen des Ausspähens von Daten lieferten die Täter eine Bekennung mit (s. Abbildung 29).

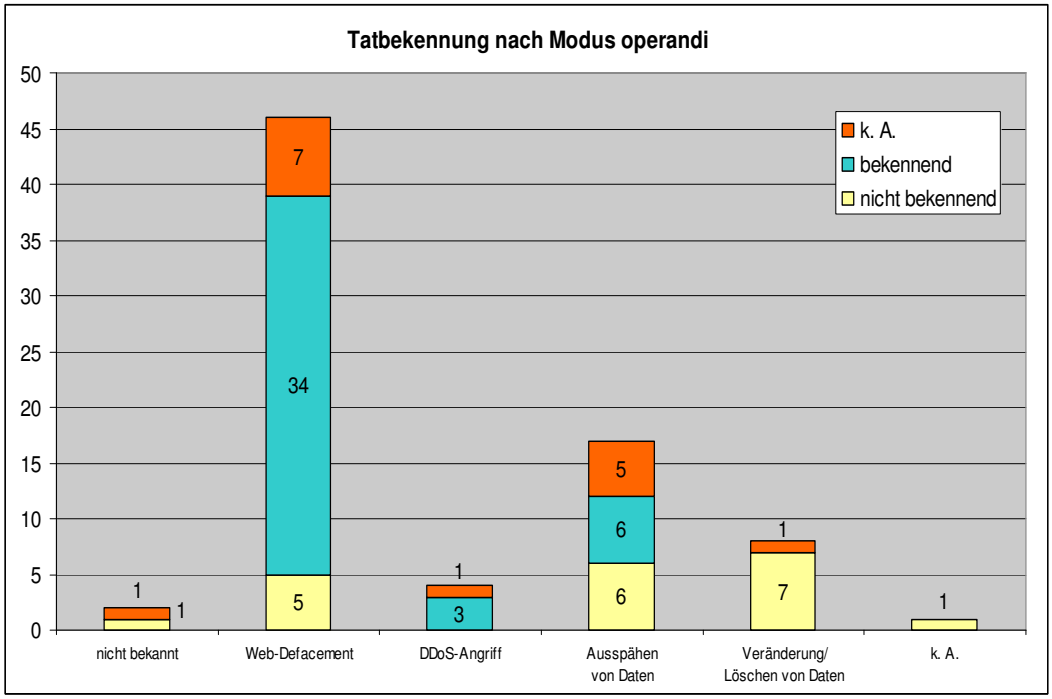


Abbildung 25: Bekennung zur Tat bezogen auf Vorgehensweise in 78 Fällen.

Die in der Fallanalyse entdeckten Gruppierungen wurden noch einmal nach dem jeweiligen Zielobjekt ausgewertet. Hier ergibt sich folgendes Bild:

Fehler! Es ist nicht möglich, durch die Bearbeitung von Feldfunktionen Objekte zu erstellen.

Abbildung 26: Hacktivistische Gruppierungen mit Angriffszielen.

Anonymous und das Ayyildiz Team weisen mit Geschädigten aus jeweils zwei unterschiedlichen Kategorien die größte Vielfalt an Zielobjekten auf.
Die Geschädigtenkategorien „Privat“ und „Wirtschaft“ wurden von den meisten unterschiedlichen Gruppierungen angegriffen, nämlich von jeweils sechs und fünf. Gefolgt von „Kirche/Verein/Schule“ die von vier unterschiedlichen Gruppierungen angegriffen wurden und „Behörde/Partei“ die Opfer von zwei Gruppen wurden.

Von den 15 in der Fallanalyse auftauchenden Gruppierungen konnten sieben mittels Internet weiter untersucht werden. So konnten für *1923 Turk Group, Ayyildiz Team, No Name Crew, Underground Nazi Hacktivist Group,Anonymous #OpBlitzkrieg, PKK* und *NMTD TIM* weitere Informationen zur Entstehung sowie zu hacktivistischen Motiven und Zielen recherchiert werden, die im Folgenden kurz vorgestellt werden:

> Die hacktivistische Gruppierung *1923 Turk Group* versteht sich als „Cyber-Armee“ der Türkei, deren Ziel es ist, das Land in der virtuellen Welt zu verteidigen.[126] Opfer ihrer Angriffe sind v. a. Websites von Organisationen und Ländern, die Israel unterstützen sowie Websites, die nach Meinung der Gruppierung unmoralische/-sittliche Inhalte enthalten.[127]
>
> Die Gruppierung *Ayyildiz Team* nimmt eine anti-europäische sowie anti-kurdische Haltung ein. Sie sieht sich selbst als im Dienste der Türkischen Nation stehend. Mitte Juni 2014 attackierte die Gruppierung den Internetauftritt des Europäischen Rates. Durchgeführte Ermittlungen der EU kamen zu dem Ergebnis, es handle sich bei der Gruppierung um türkische Nationalisten, die der EU den „Cyber-Krieg“ erklärt hätten.[128]

[126] https://www.facebook.com/1923TurkCom/info
[127] http://www.israelnationalnews.com/News/News.aspx/137819#.U5ageXgvD49
[128] http://www.focus.de/digital/computer/hacker-tuerkische-nationalisten-erklaeren-eu-den-cyber-krieg_aid_317709.html

Bei der *No Name Crew* handelt es sich um eine deutsche Hackergruppierung. Ziel dieser Hacktivisten ist es, für die Rechte und die Freiheit der Bürger zu kämpfen und insbesondere die Privatsphäre vor staatlichen Eingriffen zu schützen. Die No Name Crew griff beispielsweise im Jahr 2011 das IT-System von Bundespolizei und Zoll an und entwendete Informationen, die anschließend veröffentlicht wurden. Für Aufsehen sorgten v. a. die Informationen über das geheim gehaltene Ortungssystem „Patras" der Bundespolizei.[129]

Die *Underground Nazi Hacktivist Group* fand ihren Ursprung 2011 in New York City und ist bekannt für ihre DDos-Angriffe gegen staatliche Websites, z. B. von FBI, CIA und der Regierung der USA. Politisch treten die Underground Nazi Hacktivist Group gegen die US-amerikanischen Gesetze CISPA („Cyber Intelligence Sharing and Protect Act") und SOPA („Stop Online Piracy Act") ein.[130]

Hinter *#OpBlitzkrieg* verbirgt sich eine Operation, die durch Anonymous in Deutschland ins Leben gerufen wurde und sich gegen Webpräsenzen von Neonazis und „Nazi-Hostern" richtet. Informationen zu enttarnten Neonazis wurden hierbei auf der Internetplattform http://nazi-leaks.net veröffentlicht. Diese Website ist mittlerweile allerdings nicht mehr existent.[131]

Die Terrororganisation *PKK* entdeckte ebenfalls den Nutzen des Internets für sich und besitzt ein eigenes „Hacker-Team", welches gezielt Websites angreift und Propagandamaterial auf diesen hinterlässt. Einem solchen Angriff fiel z. B. der Internetauftritt des Türkischen Finanzministeriums zum Opfer.[132] Im Zusammenhang mit den Hackangriffen der PKK gab es bereits zahlreiche Festnahmen in der Türkei.[133]

Die Gruppierung *NMTD TIM* wurde am 09.09.2006 gegründet und besteht aus einem türkischen Hacker-Team. Die Mitglieder bezeichnen sich auf dem Facebook-Auftritt selbst als virtuelle Helden im Kampf gegen Terrorismus und Angriffe/Provokationen gegen die Republik Türkei.[134] Laut Angaben auf der Internetseite http://zone-h.org konnten der Gruppierung bereits 4234 Angriffe auf Websites zugeordnet werden (Stand 05.06.2014).

[129] http://de.wikipedia.org/wiki/No-Name-Crew
[130] http://knowyourmeme.com/memes/people/ugnazi
[131] http://www.anonpedia.net/wiki/Operation_Blitzkrieg
[132] http://www.deutsch-tuerkische-nachrichten.de/2011/11/274590/cyberwar-pkk-startet-hacker-angriff-im-internet/
[133] http://garwarner.blogspot.de/2010/03/pkk-hackers-arrested-in-turkey.html
[134] https://tr-tr.facebook.com/NMTD.T

Wegen der großen Anonymität im Cyberraum ist es nicht nur für die Strafverfolgung schwierig, Erkenntnisse über die Täter zu erlangen, sondern auch für die Forschung, generalisierbare Aussagen zu Tätern zu gewinnen. Aus den Ergebnissen der Fallanalyse und den wenigen Studien zu Hacktivisten[135] entsteht das Bild eines überwiegend männlichen Hacktivisten, der zwischen 16 und 30 Jahre alt ist und aus der mittleren Bildungsschicht stammt.

Betrachtet man die 37 Beschuldigten aus der Fallanalyse genauer, d. h. nach Geschlecht und Alter differenziert, so fällt auf, dass sich in der Altersspanne 38 bis 53 Jahre nur weibliche Beschuldigte finden lassen. Die Zahl der über 53-jährigen Beschuldigten verteilt sich auf beide Geschlechter wieder gleich, nämlich jeweils eine/r. In der Altersgruppe 14 bis 18 Jährige finden sich unter den männlichen Beschuldigten die meisten Betroffenen (14), dies gilt ebenso für den Anteil weiblicher Beschuldigter (s. Abbildung 31).

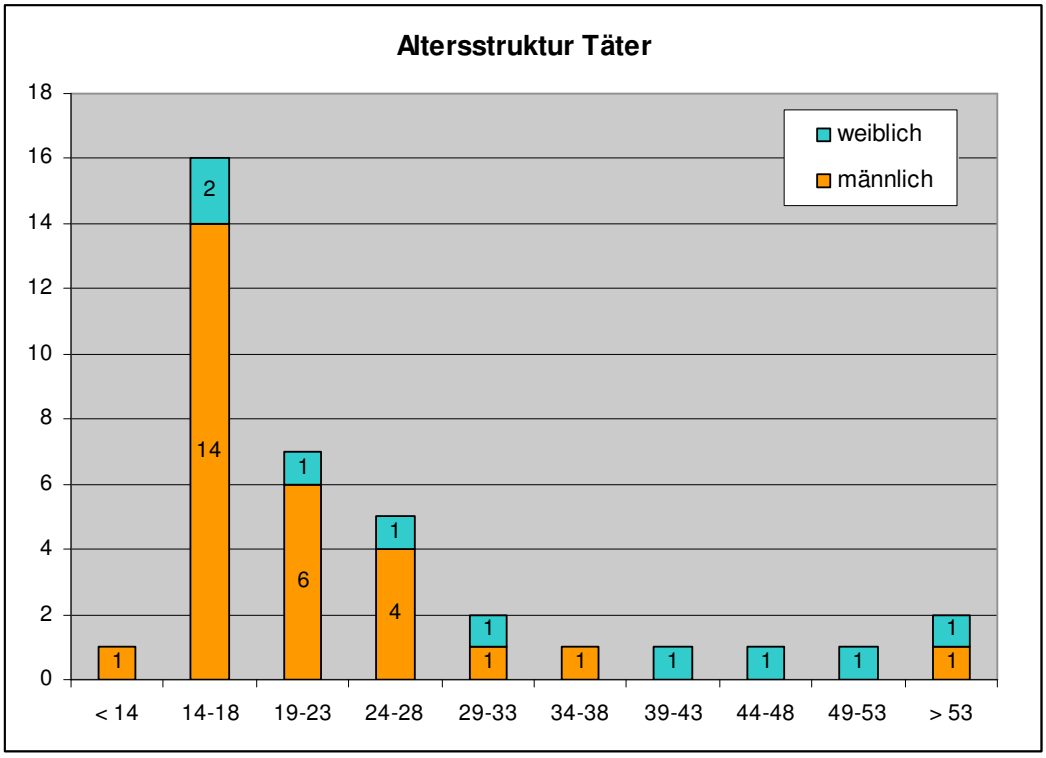


Abbildung 27: Geschlechterverteilung nach Alter bei 37 Beschuldigten.

[135] Sowie aus Studien zu Cybercrime generell, die das Phänomen Hacktivismus peripher streifen und vereinzelt Ergebnisse zum Phänomen liefern.

Da Hacktivismus letztlich nichts anderes ist als Aktivismus, der Tools und weitere Optionen des Hackings nutzt, finden sich in erster Linie Motive aus dem Bereich des Aktivismus beim Hacktivisten wieder. D. h., dass der Hacktivist sich für die Durchsetzung bestimmter ideologischer, politischer und/oder sozialer Ziele aus Bereichen wie z. B. Sozial-, Umwelt- und Wirtschaftspolitik oder Bürger- und Menschenrechte einsetzt. Seine Motivationen sind hierbei Propaganda und Protestausübung mittels IuK-Technologien und Hacking-Tools. Daneben spielen im Hacktivismus auch die Motive aus dem Bereich des Hackings eine Rolle, wie z. B. das Zusammengehörigkeitsgefühl als treibender Faktor, der Wettkampfcharakter als erster oder erste Gruppierung z. B. einen bestimmten Server lahmgelegt zu haben, Anerkennung und Respekt, Ausübung von Macht und Kontrolle, der Spaßfaktor und das *Sensation Seeking*.

In der Fallanalyse wurde eruiert, ob es möglicherweise einen Zusammenhang zwischen Motivlage und Geschädigtem gibt. Das Bild, das sich für diese Auswertung ergibt, ist jedoch sehr heterogen: Es bestehen keine signifikanten Zusammenhänge zwischen Motivation und Geschädigtem. Die Motive Protest, Propaganda, Übung und Wettbewerbsverhinderung sind über die Kategorien der Geschädigten breit verteilt (s. Abbildung 32).

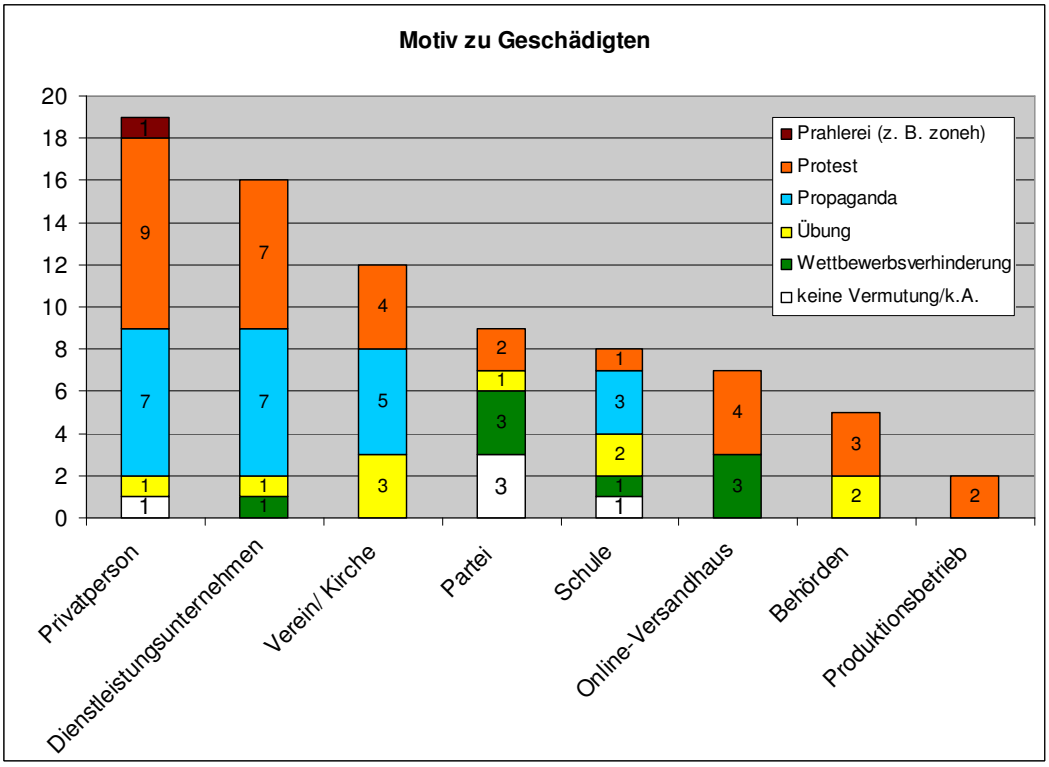


Abbildung 28: Tatmotiv bezogen auf Geschädigte in 78 Fällen.

Ein ähnlich heterogenes Bild ergibt sich, wenn man die Ergebnisse einer Kreuztabelle der Motive zu den modi operandi betrachtet:

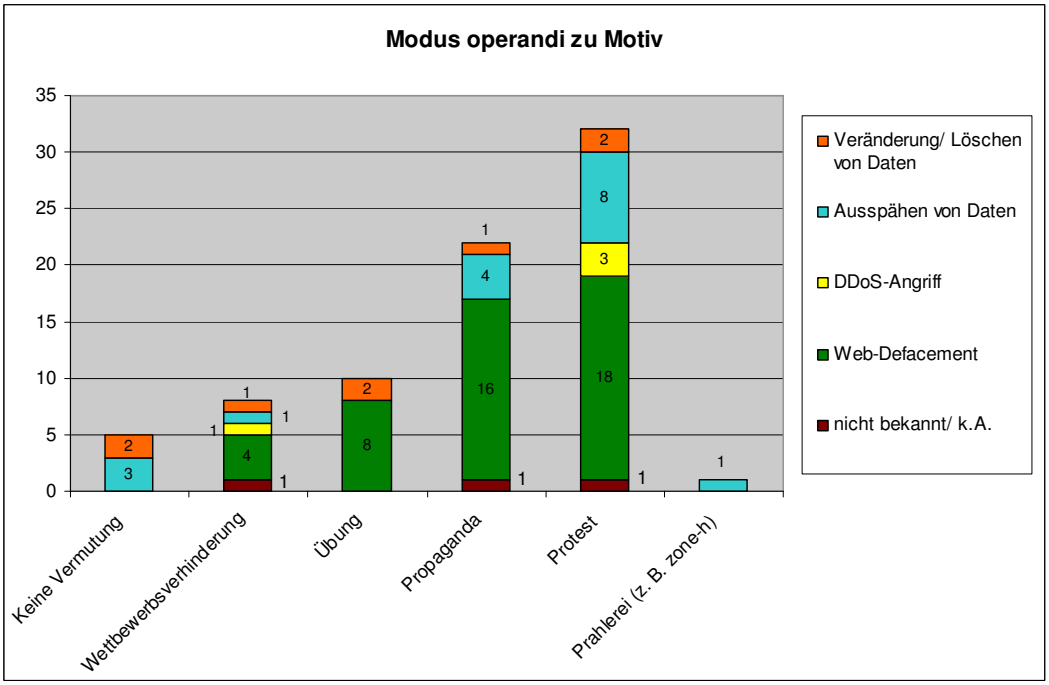


Abbildung 29: Vorgehensweise bezogen auf Motiv in 78 Fällen.

Auch hier gibt es keine signifikanten Auffälligkeiten. Für bestimmte Motive und Zwecke werden keine speziellen modi operandi gewählt. Vielmehr eignen sich die angewendeten modi operandi für alle Motivlagen der Hacktivisten und werden vermutlich eher nach Verfügbarkeit, Anwendbarkeit und Ressourcenlage ausgewählt. Insbesondere Web-Defacements eignen sich besonders für hacktivistische Motive und Zwecke wie Protest und Propaganda. Das Ausspähen von Daten wurde in den ausgewerteten Fällen als ein Teil späterer öffentlicher Diffamierungen und für Propaganda- und Protestzwecke eingesetzt.

Auch die Überlegung, dass das Hinterlassen einer Bekennung durch den/die Täter abhängig vom jeweiligen Motiv ist, wurde geprüft. Hier zeigt sich, dass insbesondere bei Propagandataten Bekennungen hinterlassen werden, was nachvollziehbar ist, da die Öffentlichkeit beeinflusst und für die Gruppe geworben werden soll (s. Abbildung 34).

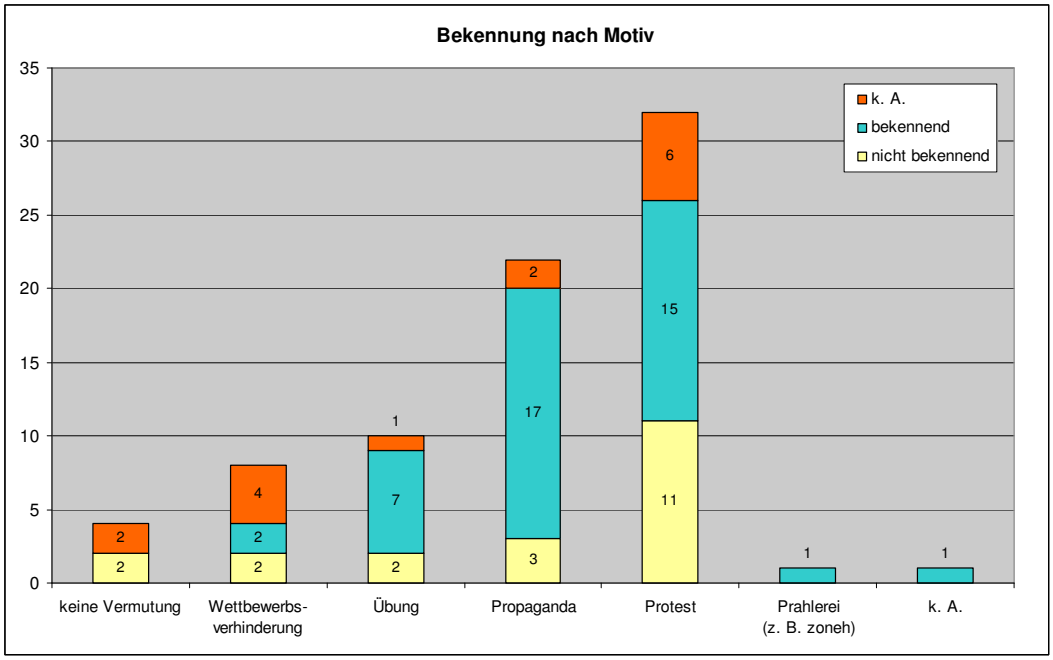


Abbildung 30: Bekennung zur Tat bezogen auf Tatmotiv in 78 Fällen.

5 Bewertung und Diskussion der Ergebnisse

5.1 Umsetzung der Projektziele

Im Ergebnis liefert das Projekt neben einer klaren begrifflichen Abgrenzung des Phänomens zu verwandten und ähnlichen phänomenologischen Strömungen eine begründete Erkenntnisbasis zum Phänomen des Hacktivismus im Hellfeld. Empirisch wurde die Erkenntnisbasis durch die Analyse registrierter hacktivistischer Fälle in Deutschland erweitert und fundiert. Die Zahl ausgewerteter Fälle (78 bereinigt[136] bzw. 183 insgesamt) erlaubt generalisierbare Aussagen zu deutschen polizeibekannten Fällen.

Mittels Sekundär- und Fallanalyse konnten für den Projektziel-Baustein *Basis-Phänomenologie* Aussagen zu Vorgehensweisen, Verschleierungstechniken und in geringerem Umfang auch zu Kommunikation gewonnen werden. Auch für den Baustein *Szene-Trend* konnten Entwicklungen und Szenedynamiken beschrieben werden. Aussagen zu Schäden ließen sich nur beispielhaft gewinnen und zusammentragen, die Repräsentativität der Schadensangaben ist hier nicht gewährleistet. Der dritte Zielbaustein strebte die Generierung von *Täter-Typologien* an. Die Datenlage sowohl der Auswertungen mittels Sekundäranalyse als auch mittels Fallanalyse erlaubte keine Konstruktion von Typologien. Es ließen sich lediglich Aussagen zu hacktivistischen Tätern registrierter Fälle gewinnen, deren Generalisierbarkeit aufgrund verschiedener Faktoren äußerst eingeschränkt ist: So handelt es sich bei den Tätern aus der Fallanalyse ausschließlich um Beteiligte eines hacktivistischen Angriffs, wobei nicht sicher ist, wie viele der Beschuldigten lediglich als Mitläufer agierten. Auch hinsichtlich der Erkenntnisse zu Tätern aus der Sekundäranalyse ist nicht verifizierbar, in welchem Maße sich diese auf tatsächliche Hacktivisten i. S. von ideologisch motivierten Personen also Aktivisten beziehen, bzw. wie stark diese Erkenntnisse durch Merkmale von Gelegenheits-Sympathisanten und/oder Mitläufern geprägt sind. Dennoch wurden Aussagen zu soziodemographischen und -ökonomischen Merkmalen sowie Motive und Zielrichtungen hacktivistischer Täter und Gruppierungen zusammengetragen und ausgewertet.

[136] 106 Fälle stammen aus einem Verfahren und wurden für viele Berechnungen (wie z. B. modi operandi) als ein Fall gezählt.

5.2 Expertenarbeitstreffen

5.2.1 Praxisbewertung der Ergebnisse

Die Teilnehmer des Arbeitstreffens bewerteten die vorgestellten Ergebnisse der Sekundär- und Fallanalyse danach, ob und inwieweit diese den Erfahrungen und Erkenntnissen aus der eigenen Praxis bzw. bisherigen Vermutungen entsprechen. Die Ergebnisse der Sekundär- und Fallanalyse lassen sich sechs Kategorien zuordnen: Modus operandi, Geschädigte, Schaden, Täter, Motive und Ideologien. In der Gesamtschau ergibt sich, dass ein Großteil der Erkenntnisse aus Sekundär- und Fallanalyse auch die (Erfahrungs-)Praxis der Experten in den sechs Kategorien widerspiegelt:

Modus operandi

Die Fallanalyse weist für die häufigsten Vorgehensweisen bei hacktivistischen Angriffen insbesondere das Web-Defacement aus, gefolgt vom Ausspähen von Daten und vom Verändern bzw. Löschen von Daten.

Das Web-Defacement wurde auch von den Teilnehmern in ihrer Praxis als von den Tätern/vom Täter meisteingesetzte Vorgehensweise wahrgenommen. Daneben spielen auch das Löschen von Daten und Webseiten eine Rolle. DDoS-Attacken tauchen in der Fallanalyse selten auf. Aus fachlicher Sicht wurde jedoch die Zahl der DDoS-Attacken als höher eingeschätzt und hier ein entsprechend großes Dunkelfeld vermutet. Begründet wurde die höhere Zahl registrierter Web-Defacement mit der größeren Wahrnehmbarkeit von Web-Defacement im Gegensatz zu DDoS-Angriffen.

Geschädigte

Die Sekundäranalyse spricht in erster Linie von Regierungen, Polizei und Unternehmen als Hauptgeschädigten. Die Fallanalyse zeichnet hier ein anderes Bild: An erster Stelle stehen Privatpersonen, gefolgt von Schulen und Unternehmen und erst an letzter Stelle finden sich Behörden. Diese Ergebnisse spiegeln jedoch nur das Hellfeld wider und unterliegen damit verschiedenen Selektionseffekten, wie z. B. dem Anzeigeverhalten.

Die Teilnehmer unterstrichen hier die Erkenntnisse aus der Sekundäranalyse: Wirtschaftsunternehmen und Firmen sowie politische Parteien seien die Hauptbetroffenen von hacktivistischen Angriffen. Privatpersonen, ehrenamtliche und sportliche Vereine sowie

Kirchen und Schulen wurden vor allem als Zufallsgeschädigte gewertet, wie z. B. durch automatisierte Web-Defacements.

Schaden

Der (wirtschaftliche) Gesamtschaden durch hacktivistische Angriffe lässt sich nur schätzen. Differenzierte und belastbare Aussagen gibt es hierzu nicht, was zum Teil auch an dem niedrigen Anzeigeverhalten der Geschädigten (hier insbesondere Unternehmen) liegt. Hinzu kommt die Schwierigkeit der Messbarkeit und Abschätzbarkeit von nur bedingt mittelbaren Schäden wie z. B. Reputationsverlusten und Imageschäden.

Auch die Teilnehmer machten die Erfahrung, dass Schäden häufig unbekannt, uneinheitlich und auch zum Teil unerheblich seien. Für Web-Defacements wurde das finanzielle Schadenspotenzial als eher gering eingestuft. DDoS-Attacken und Datenlöschung (vor allem bei Banken) verursachen hier höhere finanzielle Schäden.

Es wurde vermutet, dass der Täter am materiellen Schaden häufig gar nicht interessiert sei und diesen, wenn er eintritt (z. B. als Kollateralschaden), auf eine ideelle Ebene (z. B. bei Behörden) transferiere. Finanzielle Einbußen, die dem Geschädigten z. B. für die Instandsetzung des Systems entstehen, würden für die Täter quasi wie eine zusätzliche ideologische Bestrafung funktionieren.

Täter

Die Fallanalyse ergibt, dass der Täter in den meisten Fällen unbekannt ist, was von den Teilnehmern des Workshops unterstrichen wurde. Die Vermutungen der Teilnehmer zu soziodemographischen Merkmalen bekannter Tätern entsprechen ebenfalls den Ergebnissen der Sekundäranalyse, nämlich dass der Täter in 90% der Fälle männlichen Geschlechts und zwischen 18 und 30 Jahren alt ist. Daneben wurde die Vermutung geäußert, dass ein Großteil der Täter überwiegend islamischen/islamistischen Gruppierungen angehöre. Es wurde auch festgehalten, dass es nur eine geringe Anzahl von Tätern im inneren Kern hacktivistischer Gruppierungen geben könne, die über die nötigen technischen Kenntnisse verfügen. Ferner wurde vermutet, dass es sich bei den Hacktivisten (insbesondere den technisch versierten) überwiegend um die „üblichen“ Cybercrimetäter handele, die quasi „nebenbei“ hacktivistische Angriffe (planen und) ausführen. Zudem wurden viele Mitläufer vermutet, die sich unter Umständen auch mit den hacktivistischen Zielen identifizieren können. Des Weiteren bestand eine Mutmaßung darin, dass die Täter auch nachrichtendienstlich bzw. staatlich gelenkt würden.

Motive

Sowohl Sekundär- als auch Fallanalyse zeigen, dass die Hauptmotive mit denen hacktivistische Taten begangen werden, Propaganda und Protest sind. Dies wurde auch von den Teilnehmern so gesehen. Daneben spielen jedoch auch der Spaßfaktor („for the lulz“)[137] sowie die Verhinderung von Wettbewerb und von politischen Maßnahmen (wie z. B. Aussagen, Informationen im digitalen Bereich) im Wahlkampf eine Rolle. Als weiteres Motiv wurde vermerkt, dass der Adressat durch die hacktivistische Tat wirtschaftlich und/oder politisch geschwächt werden solle.

Ideologien

Aussagen zu Ideologien lassen sich häufig nur über die Interpretation der Inhalte von Web-Defacements und anderen mit der Tat verknüpften Statements ableiten. Die Erkenntnisse aus der Fallanalyse zu hacktivistischen Taten durch türkische bzw. ausländische Nationalisten sowie islamische/islamistische Gruppierungen wurden von den Teilnehmern bestätigt. Daneben bestanden jedoch auch die Vermutungen, dass hacktivistische Aktivitäten nicht immer ideologisch geprägt sein müssen: So handele es sich häufig um Mitläufer, die dem Hype folgen, um Hacker, die sich einen Namen machen wollen oder aber es stecke, insbesondere bei behördlich gelenkten Tätern, ein staatliches Interesse hinter den Taten.

5.2.2 Erweiterte Betrachtung des Phänomens

Für die Bearbeitung des Phänomens Hacktivismus in seinen unterschiedlichen Kontexten wurden für das Expertenarbeitstreffen vier Aspekte herausgearbeitet, die zwar nicht allumfassend jedoch wesentlich bei der Betrachtung und Diskussion des Phänomens sind: Dunkelfeld, Hemmschwelle, Erfassen von Hacktivismus und Gefährdungspotenzial.

Dunkelfeld

Die Größe des Dunkelfelds ist immer abhängig vom jeweiligen Delikt und Phänomenbereich. Für Cybercrime allgemein wird das Dunkelfeld als relativ groß eingeschätzt. Die Teilnehmer fanden Thesen sowohl für ein großes Dunkelfeld im Bereich Hacktivismus als auch für ein großes Hellfeld in diesem Phänomenbereich:

Wenn ein Angriff vom Geschädigten nicht festgestellt wird, vom Geschädigten nicht angezeigt wird oder nachfolgende Bekennungen bzw. Publikationen des Täters/der Täter zum

[137] „for the lulz“ = zum Spaß; Motto insbesondere der „4chan/b“-Gemeinde und von LulzSec.

Angriff keinem tatsächlichen Angriff zugeordnet werden können, dann sei davon auszugehen, dass das Dunkelfeld in diesem Phänomenbereich relativ groß sein muss.
Besteht die Intention darin, Protest und Propaganda in einer öffentlichkeitswirksamen Art auszuüben, dann sei von einem großen Hellfeld auszugehen.[138]

Bei den Überlegungen zu den Erschließungsmöglichkeiten des Dunkelfelds taten sich etliche Ideen aber auch Schwierigkeiten auf, die es bei der Konstruktion und Umsetzung von Methoden zu berücksichtigen gelte:
Um mehr über die hacktivistischen Aktivitäten und Taten zu erfahren, die bislang im Dunkelfeld geblieben sind, wurden Unternehmensbefragungen, Täterbefragungen und teilnehmende Beobachtungen vorgeschlagen. Da Taten vom Geschädigten zum Teil unbemerkt bleiben oder dieser das konkrete Delikt nicht erkennen bzw. benennen kann, wurde empfohlen, durch Öffentlichkeitsarbeit potentielle Geschädigte bezüglich möglicher Zeichen einer Tat zu sensibilisieren. Um Geschädigte dazu zu bringen Taten anzuzeigen bzw. zu melden, solle eine Meldepflicht (wie z. B. in Form des geplanten IT-Sicherheitsgesetzes) eingeführt werden. Ein entsprechender Vorstoß hinsichtlich der Meldepflicht von Unternehmen bei schwerwiegenden Angriffen wurde bereits unternommen. Eine allgemeine Meldepflicht im Rahmen der Straftaten der §§ 303 a, b, c StGB wird jedoch kaum als realisierbar angesehen.
Bei der teilnehmenden Beobachtung stelle sich häufig die Frage nach dem Zugang zur entsprechenden Szene. Umgesetzt werden könne die teilnehmende Beobachtung dann durch ein Mitlesen von Forenkommunikation und Plattformeinträgen. Allerdings steht zur Debatte, ob dies in rechtlicher Hinsicht, d.h. sowohl straf- als auch zivil-/haftungsrechtlich, realisierbar ist.

Hemmschwelle und kriminogene Faktoren

Kriminologisch betrachtet existieren unterschiedliche Faktoren, die ein kriminelles Handeln im Netz und mittels Hacking-Tools begünstigen. Einer dieser sog. kriminogenen Faktoren im Cyberraum sei vor allem der hohe Grad an Anonymität, der Strafverfolgung schwierig mache und die Chance, ermittelt zu werden, deutlich verringere und damit auch die Hemmschwelle, Straftaten im Netz zu begehen, senke. Neben dem Faktor der Anonymität und dem damit

[138] Die Analyse des Hellfeldes hat bei der Auswertung gezeigt: Protest und Propaganda sind die am häufigsten auftauchenden Motive.

verbundenen geringen Entdeckungsrisiko führten die Teilnehmer dieser Arbeitsgruppe noch weitere kriminogene und die Repression einschränkende Faktoren an:
Durch die nicht-physischen Tatmittel und die – auch rechtlich bedingten – relativ kleinen Zeitfenster zur Straftatverfolgung sei die Beweisführung beträchtlich erschwert. Die Distanz zum Opfer und ein mangelndes Unrechtsbewusstsein begünstigen Taten im Netz, wie z. B. auch die Partizipation an hacktivistischen Aktivitäten. Zudem wurde vermutet, dass auch das „gewohnte Umfeld" – das Netz – und die dort üblichen Handlungen sowie das gewohnte Verhalten im Netz die Hemmschwelle für inkriminierte Aktivitäten senken können, da es vom Surfen zum DDoS-Angriff quasi nur „ein paar Klicks" sind, nach dem Motto: „Vom Internetnutzer zum Hacktivisten!?" Es wurde auch über die Hemmschwelle zu anderen Cybercrime-Delikten diskutiert, quasi: „Vom Hacktivisten zum Terroristen, Phishing-Delinquent oder gar zum IT-Sicherheitsberater!?" Hier zeichnet sich allerdings (bislang) keine lineare Entwicklung ab.

Die Teilnehmer leiteten aus den vorangegangenen Überlegungen Implikationen ab:

An erster Stelle stand die Aufforderung zu verdeutlichen, dass sich die Teilnahme an Straftaten im Netz wie dem Hacktivismus nicht lohnen dürfe. Hier müssen vor allem die Strafverfolgungsbehörden in die Pflicht genommen werden, Cybercrime-Delikte konsequent zu verfolgen. Hinsichtlich der technischen und personellen Ressourcenlage ist bundesweit durch die Einrichtung von Fachdienststellen bei Polizei und Justiz bereits eine positive Entwicklung zu verzeichnen. Auch auf internationaler Ebene werden zukünftig mit dem Auf- und Ausbau entsprechender Institutionen (EC3, IGCI) stärkere Kooperationen und damit einhergehend eine effektivere Bekämpfung der Cybercrime zu erwarten sein. Zur Erreichung dieses Ziels ist es jedoch notwendig, Defizite auf dem Gebiet der nationalen Rechtslage als auch rechtliche Probleme im Bezug auf den internationalen Informationsaustausch bzw. der internationalen, grenzüberschreitenden Zusammenarbeit zu beheben. Gerade die aktuelle Rechtsprechung des EuGH zur Rechtmäßigkeit der Vorratsdatenspeicherung stellt jedoch einen Rückschritt in diesem „gesetzlichen Harmonisierungsprozeß" dar.
Die Nutzer- und (potentielle) Täterseite solle bezüglich der Strafbarkeit solcher Taten im Netz sensibilisiert werden, z. B. durch Medienkampagnen; die Akzeptanz solcher Taten solle verringert werden. Obwohl die Strafverfolgungsbehörden durch eine aktive Pressearbeit im Rahmen der Berichterstattung zu operativen Großereignissen zu einer solchen Sensibilisierung beitragen, wird die generelle Zuständigkeit für diesen Bereich vornehmlich

bei nicht polizeilichen Behörden (BSI), Institutionen (NGO) bzw. Arbeitskreisen (wie z. B. dem Programm Polizeiliche Kriminalprävention der Länder und des Bundes, kurz ProPK) gesehen.

Daneben solle aber auch die Eigenverantwortung der Nutzer und potentieller Opfer gesteigert werden. Es solle eine verstärkte „Awareness" d. h. Risikowahrnehmung auf Nutzerseite entwickelt werden. Angedacht werden könne auch eine Eigenverpflichtung die den Nutzern im Umgang mit dem Netz auferlegt werde, d. h. der Nutzer soll für die Sicherheit seines Computers, seiner Webseiten und seiner Daten selber verantwortlich sein. Dieser Ansatz findet sich ebenfalls in den Handlungsempfehlungen wieder, die 2009 im Rahmen der Strategie zur Bekämpfung der IuK-Kriminalität entwickelt wurden.

Für den Bereich der Strafverfolgung und Strafzumessung kamen zum einen die Vorratsdatenspeicherung zur Sprache und zum anderen der verstärkte Einsatz von Nebenfolgen wie z. B. die Einziehung des Rechners. Hier bietet auch das Jugendgerichtsgesetz einen entsprechend großen Spielraum. Der Täter-Opfer-Ausgleich wurde als weitere Möglichkeit angesehen, den Täter und die Tat aus der (kriminogenen) Anonymität zu bringen und dazu eventuell sogar noch durch fachliches Know-How des Täters den Geschädigten zu entschädigen und z. B. bei der Behebung von Sicherheitslücken zu unterstützen. Daneben wurden Überlegungen angeführt, dass Providern rechtliche Verpflichtungen auferlegt werden sollten: Dies könne in der Gestalt erfolgen, dass angeschlossene Systeme beim Nutzer (dem Endkunden) auf Sicherheit überprüft werden müssen, um bei einem unsicheren Status solange offline geschaltet zu werden, bis das Sicherheitsrisiko vom Systemverantwortlichen behoben wurde. Fraglich ist jedoch, inwieweit sich diese Verpflichtungen rechtlich umsetzen lassen.

Erfassen von Hacktivismus

Neben der statistischen Erfassung von Hacktivismus spielen auch die definitorische und die rechtliche Erfassung eine wichtige Rolle im Umgang und bezüglich der Verfolgung dieses Phänomens. In dieser Arbeitsgruppe wurde festgehalten, dass eine klare definitorische Abgrenzung des Phänomens die Grundlage für alle weiteren Erfassungsarten bilde.[139] Bei der rechtlichen Erfassung wurde festgehalten, dass es für Hacktivismus keines neuen Straftatbestandes bedürfe, sondern dass die bestehenden Straftatbestände geeignet seien,

[139] Die Definition von Hacktivismus wie sie in dem Projekt „Hacktivisten" und auch in dem Arbeitsreffen verwendet wird bzw. wurde, entspricht der geläufigen wissenschaftlich und praktisch gestützten Definition des Phänomens.

dieses Delikt mit abzudecken. Worüber aus Sicht der Arbeitsgruppe weiter diskutiert werden müsse, sei die Ausschöpfung und ggf. eine Anpassung des Strafrahmens für dieses Deliktsfeld. Für die statistische Erfassung wurden verschiedene Aspekte diskutiert und Vorschläge vorgebracht:

Die Teilnehmer waren sich einig, dass die statistische Erfassung für den Bereich der Cybercrime-Straftaten momentan generell wenig differenziert sei und dies einen Mangel im o. g. Sinne darstelle. Die Polizeiliche Kriminalstatistik (PKS) aber auch der Kriminalpolizeiliche Meldedienst (KPMD) sollen neue Parameter aufnehmen, die der Differenzierung und Spezifizierung von Delikten dienen, wie z. B. durch einen Marker „Cybercrime“ und durch die Unterscheidung von wirtschaftlichen und politischen Motiven. In diesen Bereichen sind jedoch schon einige Fortschritte zu verzeichnen: Nach Festlegung einer bundesweit gültigen Definition „Cybercrime“ wurden neben dem Sondermeldedienst Cybercrime auch die Verbundanwendung Inpol-Fall Cybercrime und die PKS angepasst und u. a. ein Marker „Cybercrime“ eingeführt. Die Unterscheidung zwischen wirtschaftlichen und politischen Motiven gestaltet sich bei der Erstbefassung mit einem Cybercrime-Sachverhalt jedoch nicht selten schwierig, da oftmals die subjektive Zielrichtung der Täter nicht klar erkennbar ist. Cybercrime-Sachverhalte mit PMK-Bezug fallen bereits heute in die Zuständigkeit von Staatsschutz-Dienststellen, was sich in den zu bedienenden Meldediensten niederschlägt.

Weiterhin wäre die Intensivierung einer differenzierten statistischen Erfassung auch durch die Erhellung des Dunkelfelds möglich.

Daneben wurden, unabhängig von PKS und KPMD, verschiedene Ansätze statistischer Erfassung vorgeschlagen:

- Ein quantitativer Ansatz, der z. B. Angriffe zählt;
- Ein qualitativer Ansatz, der Aussagen über Täter trifft und damit eine Messbarkeit der Auswirkung im politischen Raum ermöglicht (z. B. bei sog. Shitstorms);
- Ein schadensbezogener Ansatz, der finanzielle Verluste erfasst
- und ein technischer Ansatz, der Aussagen über die Verfügbarkeit von Tools für z. B. DDoS, Hacks, Phishing etc. trifft.

Für eine Umsetzung der vorgeschlagenen Ansätze müsse jedoch geklärt werden, welches zentrale statistische Erfassungssystem herangezogen werden solle, woher verlässliche Daten zur Erfassung stammen können und wie Erfassungsfehler vermieden werden. Außerdem stelle sich die Frage, wer bzw. wie diese zusätzlichen Massendaten im Sinne des Legalitätsprinzips polizeilich bearbeitet werden sollen.

Eine weitere Empfehlung war das Einrichten eines Cybersicherheitslage-Reports für die gesamte Bundesrepublik durch ein (zu benennendes) Institut. Und bei der Modifizierung bestehender statistischer Dienste aber auch bei der Implementierung neuer Ansätze sei es unabdinglich, dass eine bundes- und länderweit einheitliche Umsetzung der statistischen Erfassung erfolge.

Gefährdungspotenzial

Zur aktuellen Lage hacktivistischer Aktivitäten wurde in der Arbeitsgruppe einhellig festgehalten, dass derzeit relative Ruhe herrsche. Dies solle jedoch nicht dahingehend interpretiert werden, dass das Phänomen an Bedeutung verliert. Auch die sprichwörtliche Ruhe vor dem (nächsten) Sturm könne dahinterstecken, wie die Erkenntnisse aus vergangenen hacktivistischen Perioden gezeigt haben.

Das Gefährdungs- und Schadenspotenzial hacktivistischer Angriffe war bislang immer abhängig vom Zielobjekt und der vom Täter genutzten Vorgehensweise. Dies werde auch in Zukunft so bleiben, es zeichne sich jedoch ab, dass sich Hacktivismus zunehmend in Form von „combined attacks“ zeigen werde, in denen sich Experten mit „Hacking-Skills“ mit Experten im Bereich Social Engineering zusammen tun und verstärkt über soziale Medien (social media) Unternehmen angreifen werden.[140] Ein hohes Gefährdungs- und Schadenspotenzial hacktivistischer Aktivitäten werde für Angriffe auf kritische Infrastrukturen gesehen, die es so bislang aber noch nicht gegeben habe. Ein weiteres Gefährdungspotenzial von Hacktivismus sieht die Arbeitsgruppe in dem „Überschwappen“ des Phänomens auf den Bürger bzw. Internetnutzer: Um an einer „Demo“ teilzunehmen, genüge ein einfacher Mausklick. Den meisten Nutzern sei in dem Moment nicht klar, dass sie mit dem damit ausgelösten DDoS-Angriff eine Straftat begehen.[141]

Als Implikationen ließe sich aus diesen Überlegungen zum Potenzial von Hacktivismus ableiten, dass Unternehmen, die social media einsetzen, auch eine entsprechende Kompetenz im Umgang mit auftretenden Konflikten vorweisen müssen, damit solche Situationen nicht in hacktivistischen Angriffen münden. Die Risikowahrnehmung und die Medienkompetenz der Bürger und Internetnutzer müsse dahingehend ausgeprägt werden, dass klar werde, welche Taten im Internet strafbar sind. Funktionierende Public Private Partnerships und andere

[140] Dies zeichnet sich bereits bei Shitstorms ab, aus denen sich Verabredungen zu Angriffen hacktivistischer Natur ergeben können.
[141] Siehe hierzu auch die Ergebnisse der Arbeitsgruppe zur „Hemmschwelle“.

nationale sowie internationale Kooperationen sollen implementiert werden, um Angriffen gezielt begegnen zu können bzw. um in diesen ermitteln zu können.
Hacktivismus – ebenso wie andere Cybercrime-Phänomene – berge aber auch ein positives Potenzial, wenn z. B. Sicherheitsbehörden technisch versierte Hacktivisten für sich gewinnen können oder wenn im Rahmen von z. B. Täter-Opfer-Ausgleichen[142] geholfen werden kann, Sicherheitsrisiken aufzuzeigen und zu minimieren. Daneben solle auch diskutiert werden, inwieweit sich das Grundrecht auf Demonstrationsfreiheit im digitalen Raum durchsetzen lasse, ohne dabei Schaden zu verursachen.

5.2.3 Risikofaktoren im Umgang mit Hacktivismus und Cybercrime allgemein

Zum Abschluss des Arbeitstreffens überlegten die Teilnehmer in Form eines negativen Brainstormings, was passieren müsse, damit die Lage um Hacktivismus und Cybercrime allgemein so bleibe wie sie ist bzw. sich zukünftig noch verschlimmere. Hiermit lassen sich zum einen die von den Experten empfundenen Missstände im Umgang mit dem Phänomen aufzeigen und zum anderen lassen sich aus den Punkten des negativen Brainstormings Forderungen und Empfehlungen für Veränderungen ableiten.

Insbesondere die Experten aus dem Bereich der Strafverfolgung rückten die Rechtsproblematik in den Fokus und forderten eine rechtliche Anpassung der Strafgesetze und Strafprozessregelungen sowohl auf nationaler als auch auf internationaler Ebene, damit Cybercrime wirkungsvoll begegnet werden könne. Dazu gehören auch die Vorratsdatenspeicherung und die Quellen-TKÜ. Vorhandene Straftatbestände im Bereich Cybercrime dürfen nicht entschärft werden und die Ermittlungsbehörden sollen die Möglichkeit zur Anonymisierung und zum Einsatz verdeckter Maßnahmen haben.

Daneben wurde von allen Teilnehmern die personelle und materielle Ausstattung unterstrichen: Es bedürfe der entsprechenden quantitativen und qualitativen IT-Ausstattung, angefangen bei einer modernen Bürokommunikation bis hin zu spezialisierten Auswerte- und Forensiktools, die dem neuesten Stand entsprechen. Außerdem müsse auch qualifiziertes Personal den relevanten Bereichen zur Verfügung stehen, wozu gehöre, dass sich Aus- und Fortbildungsangebote an den Spezifika der Cybercrime-Phänomene orientieren.

[142] Siehe hierzu den Punkt „Hemmschwelle“.

Auch die Kooperation und Vernetzung mit Unternehmen, Behörden und anderen Institutionen auf nationaler, internationaler sowie interdisziplinärer Ebene wurde für die wirksame Bekämpfung von Cybercrime als wichtig und ausbaufähig bewertet. Rechtshilfeersuchen müssen schneller und effektiver (auf beiden Seiten) umgesetzt werden.

Des Weiteren werden zersplitterte Zuständigkeiten in der Bekämpfung von Cybercrime sowie die Förderung der Anonymisierungs- und Verschlüsselungstechnologien langfristig als Risiko in der erfolgreichen Verfolgung von Cybercrime-Delikten gesehen. Präventionsarbeit dürfe nicht aufgegeben werden und solle sich fortlaufend an den Ergebnissen interdisziplinärer Forschungsarbeiten zu Cybercrime stützen.

6 Fazit

Das Projekt wurde mit dem Ziel initiiert, die Erkenntnisse zum Cybercrime-Phänomen Hacktivismus zu erweitern und auf eine fundierte Wissensbasis zu stellen. Mittels Sekundäranalyse vorhandener Fachliteratur und Studien zum Forschungsgegenstand sowie mittels Fallanalyse polizeilich registrierter hacktivistischer Fälle aus dem deutschen Raum konnten neue Ergebnisse und Zusammenhänge gewonnen sowie vorhandene Aussagen differenziert werden. Daneben konnten diese Ergebnisse und Zusammenhänge in einem Expertenarbeitstreffen vorgestellt, bewertet und diskutiert werden, so dass weitere Einschätzungen zur Themenproblematik und zukünftigen Entwicklung sowie themenbezogene Implikationen ausgewertet werden konnten. Neben einer begrifflichen und inhaltlichen Abgrenzung zu anderen Cybercrime-Phänomenen liegen nun auch umfängliche Erkenntnisse zur Vorgehensweise, zu den Entwicklungen und Dynamiken der Hackitivismus-Szene(n) und auch zu Schäden sowie soziodemographischen und -ökonomischen Merkmalen der Täter vor.

In der Auswertung des erhobenen Materials im Projektteil Hellfeld ließen sich keine Hinweise darauf finden, dass es bereits Angriffe von Hacktivisten auf kritische Infrastrukturen gegeben hat. Nach derzeitigem Erkenntnisstand steht die Sabotage kritischer Infrastrukturen (Energieversorgung, Verkehrssysteme, Telekommunikation, Ernährung und Gesundheitsversorgung) ideologisch nicht im Fokus von Hacktivisten. Angriffe auf kritische Infrastrukturen der Grundversorgung werden momentan eher von Cyber-Terroristen, ausländischen Geheimdiensten und „anderen“ Cyber-Kriminellen (im Rahmen von Erpressungen) erwartet. Auch islamistisch motivierte Cyber-Attacken auf kritische Infrastrukturen sind bislang weder in Deutschland noch international bekannt geworden.

Neben dem Aspekt theoretisch (und praktisch) möglicher Angriffe auf kritische Infrastrukturen durch Hacktivisten steht außer Frage, dass die IuK-Technologien sowie das Internet Aktivisten neue effektive Wirkräume und Möglichkeiten eröffnen. Nicht nur Aktionen können schneller geplant und durchgeführt werden, auch das Zielspektrum möglicher Sympathisanten ist mit der hohen Akzeptanz und Nutzung des Internets und sozialer Medien größer, der Zugang zu Nutzern ist einfacher und ressourcensparender geworden. Auch politisch bislang wenig aktive aber interessierte Personen hätten nun die Möglichkeit, schnell und unkompliziert an entsprechenden Aktionen teilzunehmen, da

mögliche Hinderungsgründe, die mit analogen Protestformen einhergehen, wie z. B. Witterung, Anfahrt, ungewollte Entdeckungsmöglichkeit (bei ausreichender Anonymisierung des Teilnehmers), bei digitalen Aktionen nahezu ausgeschlossen sind. Daher ist zu vermuten, dass bei entsprechender Organisation und Kommunikation zur Sympathisantengewinnung hacktivistische Aktionen und Angriffe in der Zukunft nicht abnehmen werden, sondern eher zunehmen.

Auch wenn sich Hacktivismus als gesellschaftliche und demokratische Möglichkeit politischer Teilhabe etabliert, werden sich viele Aktionsformen von Hacktivismus immer auf einem schmalen Grat zwischen Aktionen zivilen Ungehorsams und illegalen Angriffen bewegen bis hin zur Grenze des Cyberterrorismus.

Der zweite Teil des Projekts „Hacktivisten“, der im ersten Quartal 2014 angelaufen ist, befasst sich mit dem Dunkelfeld in diesem Phänomenbereich. Nach der in diesem Bericht beschriebenen Aufarbeitung des Hellfelds (empirisch insbesondere für Deutschland) soll nach Möglichkeiten gesucht werden, Zugänge zum Dunkelfeld gewinnbringend zu erschließen und zu nutzen, um das Phänomen repräsentativer und genauer beschreiben zu können.

Ein umfänglicher Abschlussbericht zum Projekt Hacktivisten wird nach Beendigung des Projektteils Dunkelfeld unter Einbindung aller gewonnener Erkenntnisse erstellt.

7 Literaturverzeichnis

Alleyne, B. (2011). *We are all hackers now - critical sociological reflections on the hacking phenomenon*. In: Under Review, 1-28

Arns, I. (2002). *Netzkulturen*. Europäische Verlagsanstalt. Hamburg

Bachmann, M. (2001). *The Risk Propensity and Rationality of Computer Hackers*. In: International Journal of Cyber Criminology. Vol. 4, (1&2). S. 643-656

Bortz, J./Döring, N. (2006). *Forschungsmethoden und Evaluation für Human- und Sozialwissenschaftler*. Springer Medizin Verlag. S. 47 ff.

Brenner, S.W. (2007). *„At Light Speed": Attribution and Response to Cybercrime/Terrorism/Warfare*. In: The Journal of Law & Criminology. Vol. 97 (2). S. 379-475

Brickey, J. (2012). *Defining Cyberterrorism: Capturing a Broad Range of Activities in Cyberspace*. Im Internet: http://www.ctc.usma.edu/posts/defining-cyberterrorism-capturing-a-broad-range-of-activities-in-cyberspace

Brunsting, S./Postmes, T. (2002). *Social Movement Participation in the Digital Age: Predicting Offline and Online Collective Action.* In: Small Group Research 33: 525

Bundesamt für Sicherheit in der Informationstechnik (2012): Register aktueller Cyber-Gefährdungen und – Angriffsformen

Bühl, A. (1997). *Die virtuelle Gesellschaft*. Ökonomie, Kultur und Politik im Zeichen des Cyberspace. Westdeutscher Verlag

Carty, V./Onyett, J. (2006). *Protest, Cyberactivism and New Social Movements: the Reemergence of the Peace Movement Post 9/11*. In: Social Movement Studies, Vol. 5, 3, S. 229-249

Cole, K. A. et al. (2011). *All Bot Net: A Need for Smartphone P2P Awareness*. In: P. Gladyshv, M.K. Rogers. (Hrsg.): *Digital Forensics and Cyber Crime*. Third International ICST Conference ICDF2C 2011, Dublin, Ireland, revised Selected Papers. S. 36-46

Colemann, G. (2012). *Anonymous: Leuchtfeuer der digitalen Freiheit*. In: M. Beckedahl, A. Meister (Hrsg.). *Jahrbuch Netzpolitik 2012 – von A wie ACTA bis Z wie Zensur*. epubli GmbH, Berlin. S. 220-227

Denning, D. E. (2001). *Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy*. In: Arquilla, J./Ronfeldt, D. (eds.): *Networks and netwars: the future of terror, crime, and militancy*. RAND: National Defense Research Institute

Dreher, M./Dreher, E. (1994). *Gruppendiskussion*. In: Huber, G./Mandl, H. (Hrsg.). *Verbale Daten. Eine Einführung in die Grundlagen der Erhebung und Auswertung*. Beltz Verlag. S. 141 ff.

Dürrenberger, G./Behringer, J. (1999). *Die Fokusgruppe in Theorie und Anwendung*. Stuttgart: Akademie für Technikfolgenabschätzung in Baden-Württemberg

Fitri, N. (2011). *Democracy Discourses through the Internet Communication: Understanding the Hacktivism for the global Changing*. In: Online Journal of Communication and Media Technologies Volume: 1, Issue: 2, April 2011

Goel, S. (2011). *Cyberwarfare: Connecting the Dots in Cyber Intelligence*. In: Communications of the ACM. Vol. 54 (8). S. 132-140

Gragido, W./ Pirc, J. (2011). *Cybercrime and Espionage. An analysis of Subversive Multivector Threats*. Elsevier monographs. Amsterdam

Gröhndahl, B. (2001). *Scriptkiddies Are Not Alright*. In A. Medosch, J. Röttgers (Hrsg.): Netzpiraten. Die Kultur des elektronischen Verbrechens. S. 143 – 152. Verlag Heinz Heise. Hannover

Hampson. N.C.N. (2012). *Hacktivism: A New Breed of Protest in an Network World*. In: B.C. International & Comparative Law Review pp. 511-542. http://lawdigitalcommon.s.bc.iclr/vol35/iss2/6

Hearn, K. /Mahncke, R. /Williams, P.A. (2009). *Culture Jamming: From Activism to Hactivism*. ECU Publications

Held, W.V. (2012). *Hacktivism: an Analysis of the Motive to Disseminate Confidential Information*. Im Internet: https://digital.library.txstate.edu/handle/10877/4381

Jordan, T. (2001). *Mapping Hacktivism*. In: *Computer fraud & security*, 4, 8-11

Jordan, T./Taylor, P. (2004). *Hacktivism and Cyberwars. Rebels with a cause?* Routledge. London

Juris, J. S. (2005). *The New Digital Media and Activist Networking within Anti-Corporate Globalization Movements*. In: The Annals of the American Academy. AAPSS, 597, S. 189-208

Kaspersky. (2013). *Millionenschäden durch gezielte Cyberangriffe auf Großunternehmen*. Pressemitteilung vom 25.07.2013. Im Internet: http://newsroom.kaspersky.eu/fileadmin/user_upload/de/Downloads/PressReleases/074_PM_B2B_Targeted_Attacks_final.pdf

Kelly, B.B. (2012). *Investing in a Centralized Cybersecurity Infrastructure: Why „Hacktivism“can and should influence Cybersecurity Reform*. In: Boston University Law Review. Vol. S. 92. 1663-1711

Kochheim, D. (2010). *Cybercrime -Malware, Social Engineering, Underground Economy*. Im Internet: http://www.kochheim.de/cf/doc/Cybercrime-2010.pdf

KPMG. (2010). *e-Crime-Studie 2010. Computerkirminalität in der deutschen Wirtschaft*.
Im Internet: https://www.kpmg.de/docs/20100810_kpmg_e-crime.pdf

Lamnek, S. (1993). *Qualitative Sozialforschung. Band 2: Methoden und Techniken*. Psychologie Verlags Union.

McLaughlin, V. (2012). *Anonymous - What to fear from hacktivism, the lulz, and the hive mind?*
Im Internet:
http://pages.shanti.virginia.edu/Victoria_McLaughlin/files/2012/04/McLaughlin_PST_Thesis_2012.pdf

Medosch, A. (2001). *The Kids are out to play*. In: A. Medosch/J. Röttgers. (Hrsg.): *Netzpiraten. Die Kultur des elektronischen Verbrechens*. Verlag Heinz Heise. Hannover. S. 117-127

metac0m. (2003). *What is Hacktivism? 2.0.* Im Internet:
http://www.thehacktivist.com/hacktivism1.php

O`Rourke, S. (2011). *Empowering Protest through Social Media*. Hrsg.: School of Computer and Information Science, Security Research Centre, Edith Cowan University, Perth, Western Australia

Olson, P. (2012*). Inside Anonymous: Aus dem Innenleben des globalen Cyber-Aufstandes*. Redline Verlag. München.

Paget, F. (2012). *Hacktivismus – Das Internet ist das neue Medium für politische Stimmen*.
Im Internet: http://www.mcafee.com/de/resources/white-papers/wp-hacktivism.pdf

Raab-Steiner, E./Benesch, M. (2008). *Der Fragebogen. Von der Forschungsidee zur SPSS-Auswertung*. Facultas wuv. S. 37

Raiu, C. et al. (2012). *Kasparsky Security Bulletin 2012*. Im Internet: http://www.kaspersky.com/de/downloads/doc/kaspersky-security-bulletin-2012.pdf

Reitmann, J. (2012). *Enemy of the State*. In: Rolling Stone, Issue 1169, S. 52-62

Rheinberg, F./Tramp, N. (2006). *Anreizanalyse intensiver Freizeitnutzung von Computern: Hacker, Cracker und zweckorientierte Nutzer*. In: Zeitschrift für Psychologie. 214. 97-107

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

Slobbe, J./Verberkt, S.L.C. (2012). *Hacktivists: Cyberterrorists or Online Activists? An Exploration of the Digital Right to Assembly*. In: CoRR abs/1208.4568

SpiegelOnline. (2013). *Chinas Hacker spähen US-Militär aus*. Im Internet: http://www.spiegel.de/politik/ausland/hackerangriffe-usa-beschuldigen-china-der-cyber-spionage-a-898446.html

Taylor, P.A. (2005). *From Hackers to Hacktivists: speed bumps on the global highway*. In: New Media Society, 7, 625-646

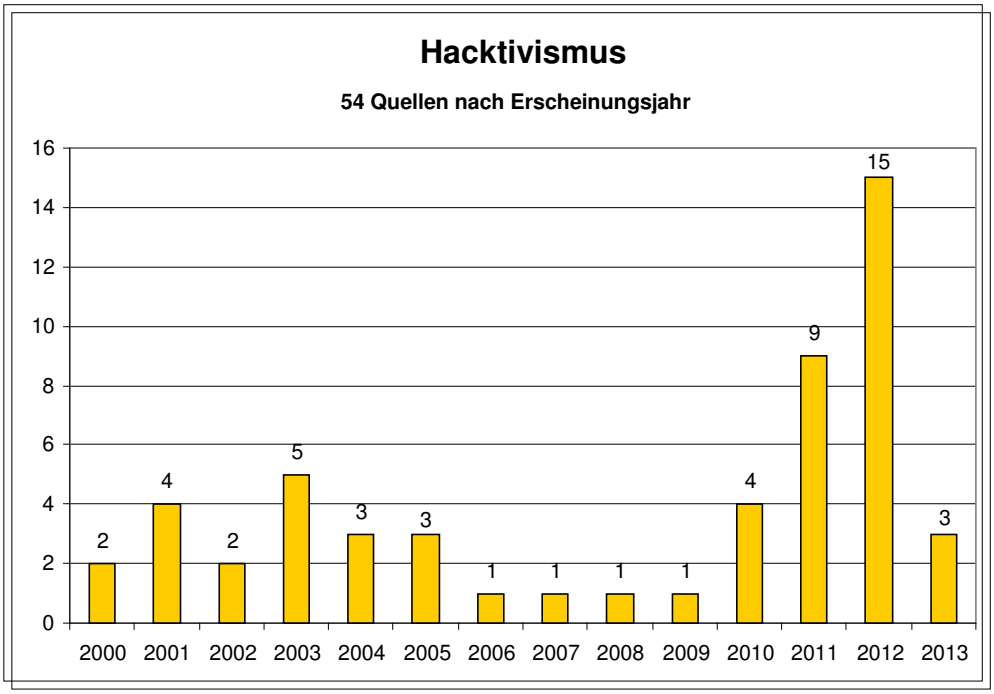
The Knightmare/Branwyn, G. (1994). *Secrets of a Super Hacker*. Loompanics Unlimited

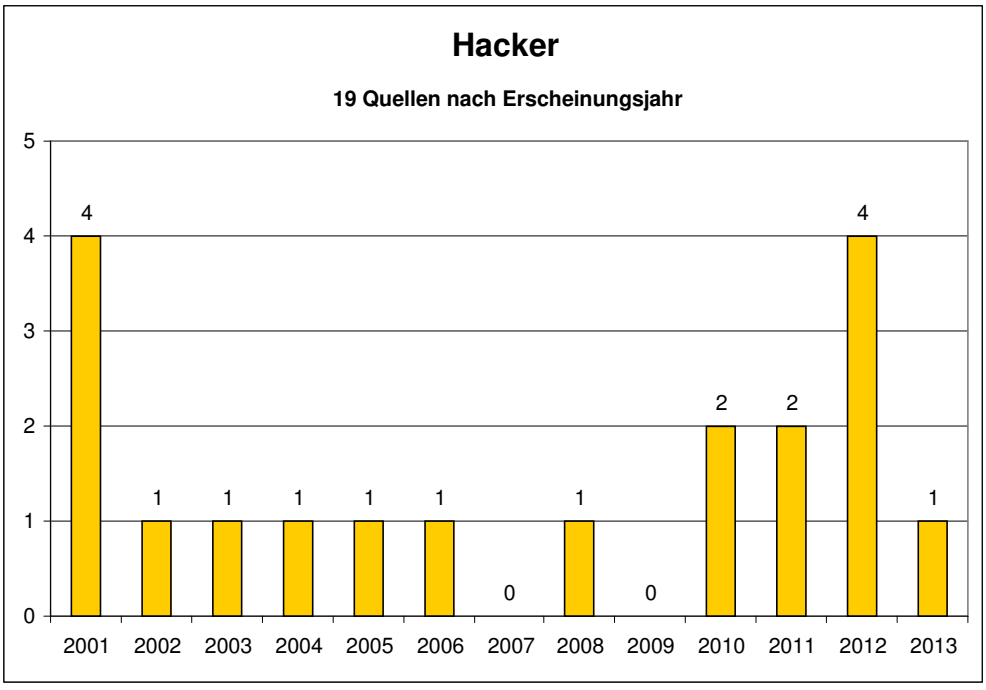
Verizon (2013). *2013 Data Breach Investigation Report*. Im Internet: http://www.verizonenterprise.com/DBIR/2013/

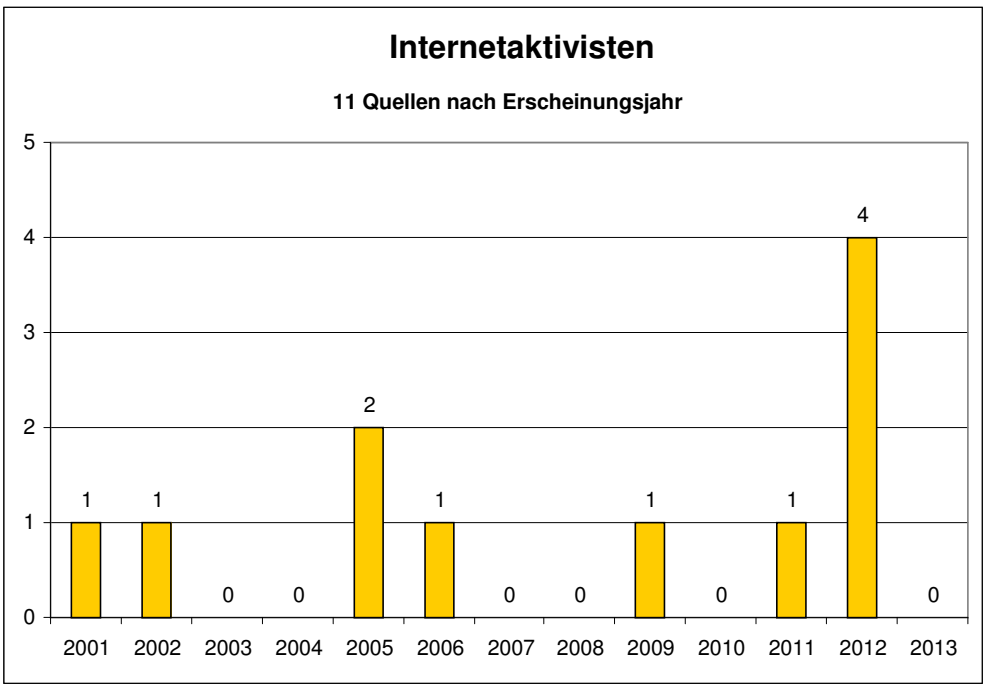
8 Anlagen

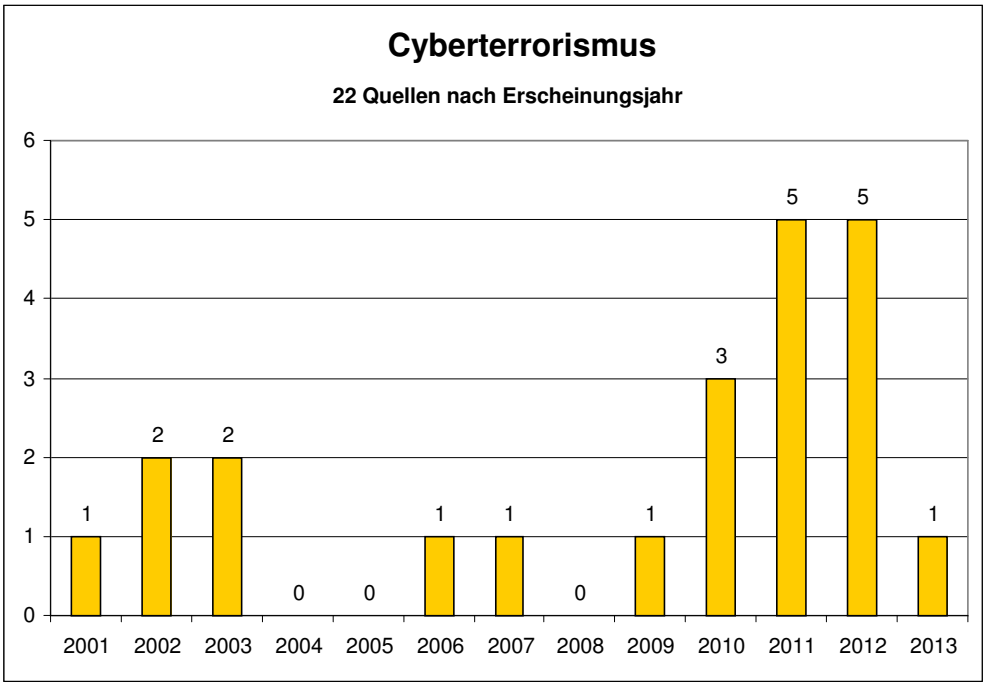
Anlage 1

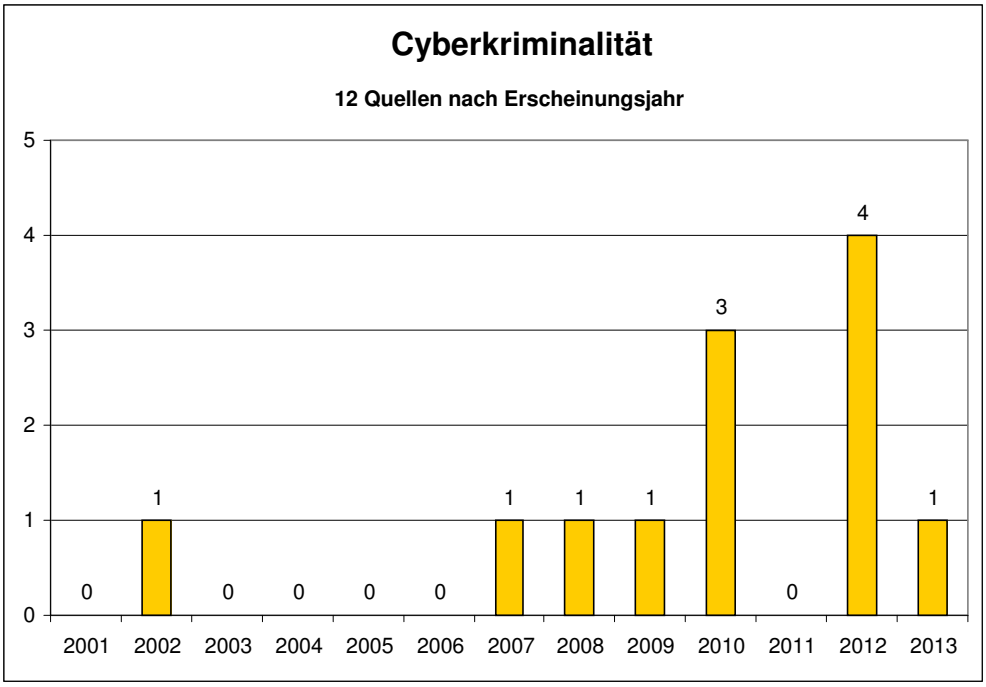
Kategorien ausgewerteter Quellen

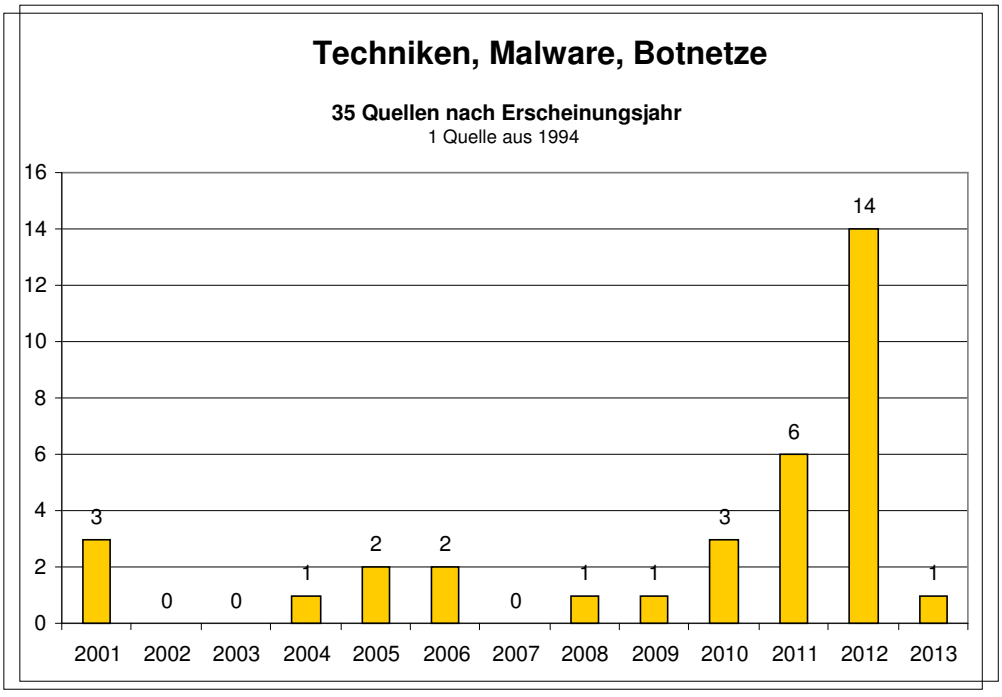


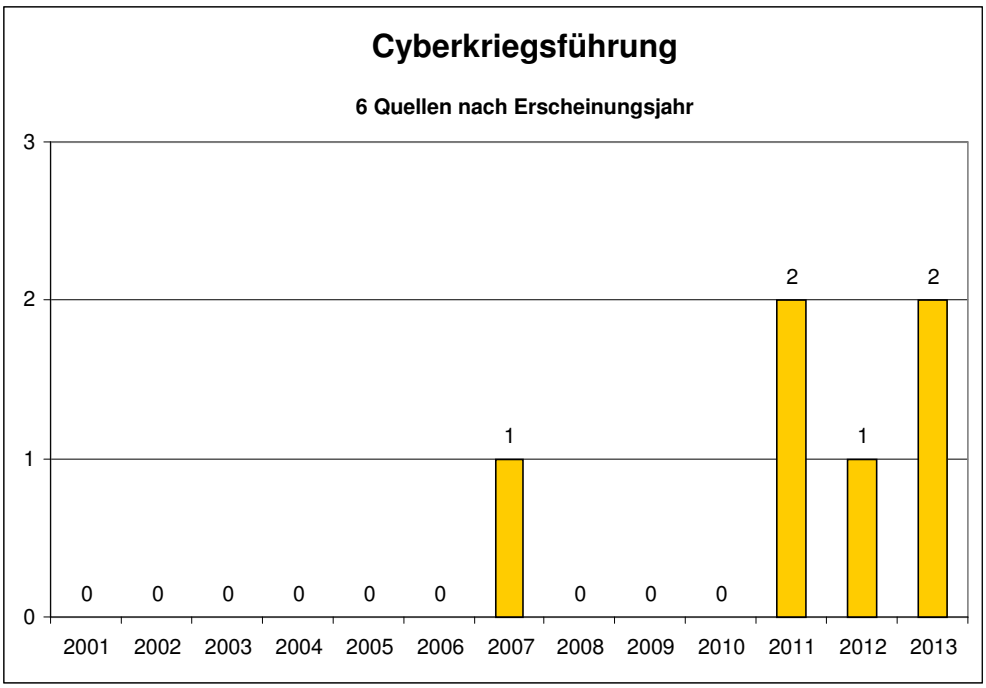


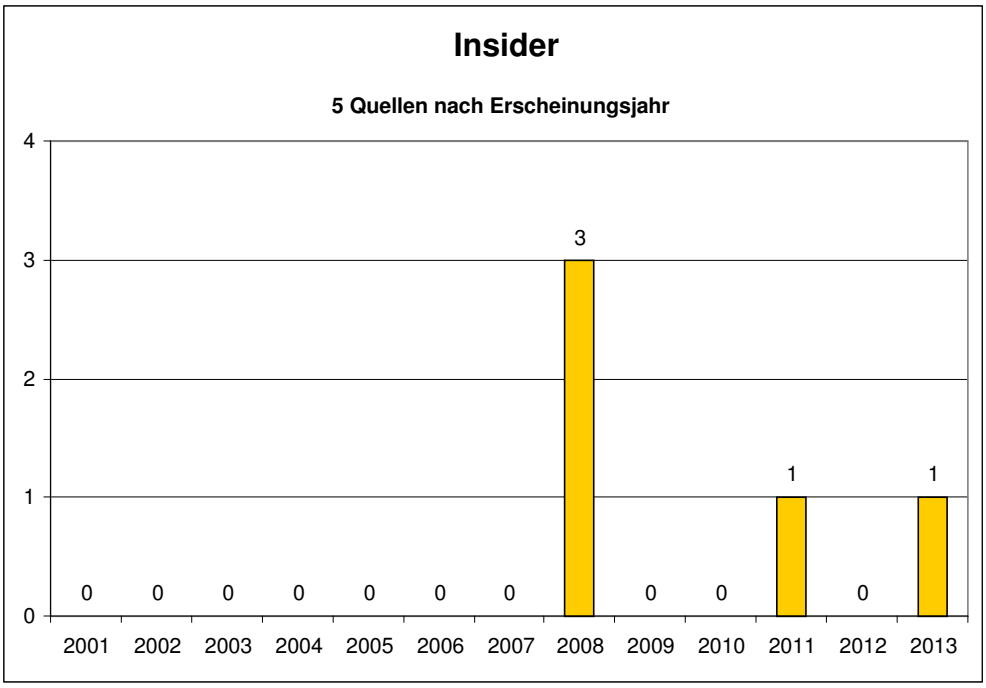

Internetaktivisten
11 Quellen nach Erscheinungsjahr
5
4
3
2
1
0
1 1 0 0 2 1 0 0 1 0 1 4 0
2001 2002 2003 2004 2005 2006 2007 2008 2009 2010 2011 2012 2013

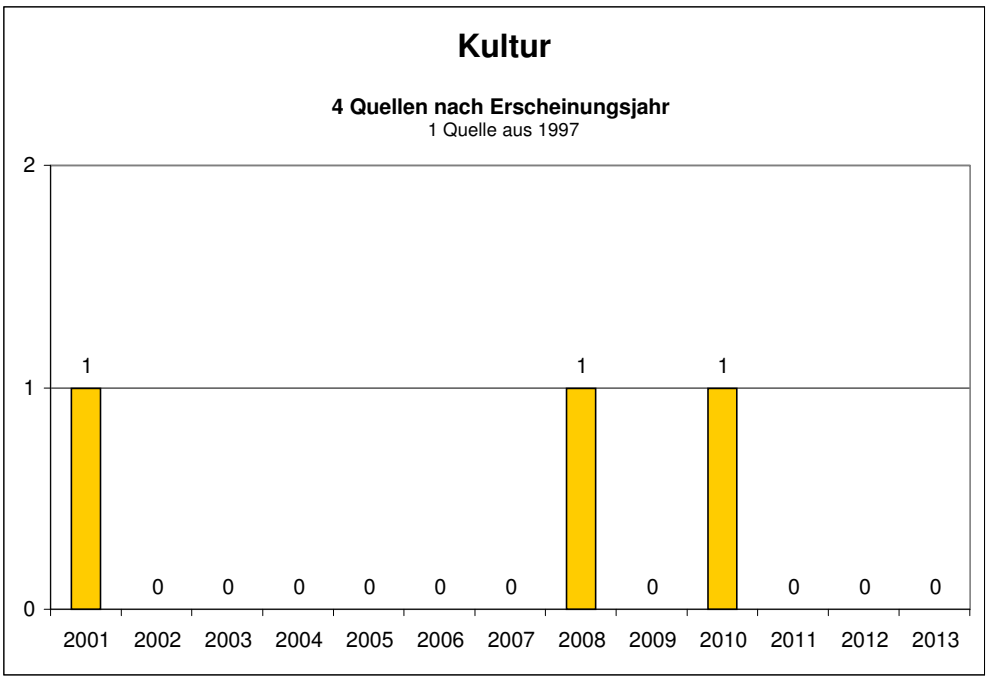

Cyberterrorismus
22 Quellen nach Erscheinungsjahr
6
5
4
3
2
1
0
1 2 2 0 0 1 1 0 1 3 5 5 1
2001 2002 2003 2004 2005 2006 2007 2008 2009 2010 2011 2012 2013

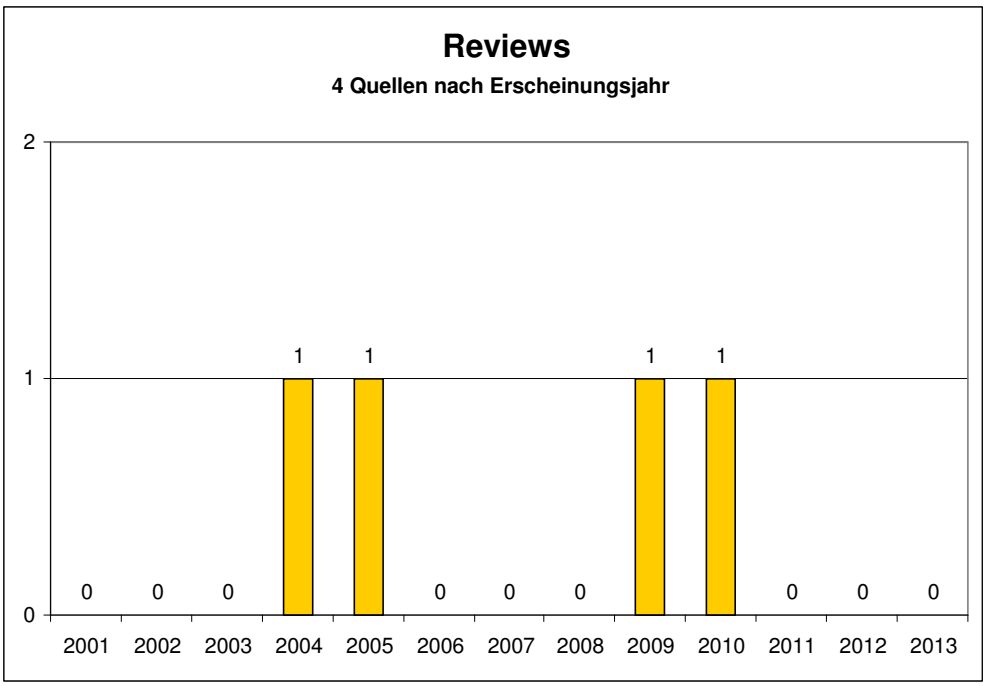

Cyberkriminalität
12 Quellen nach Erscheinungsjahr
5
4
3
2
1
0
0
1
0
0
0
0
1
1
1
3
0
4
1
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013

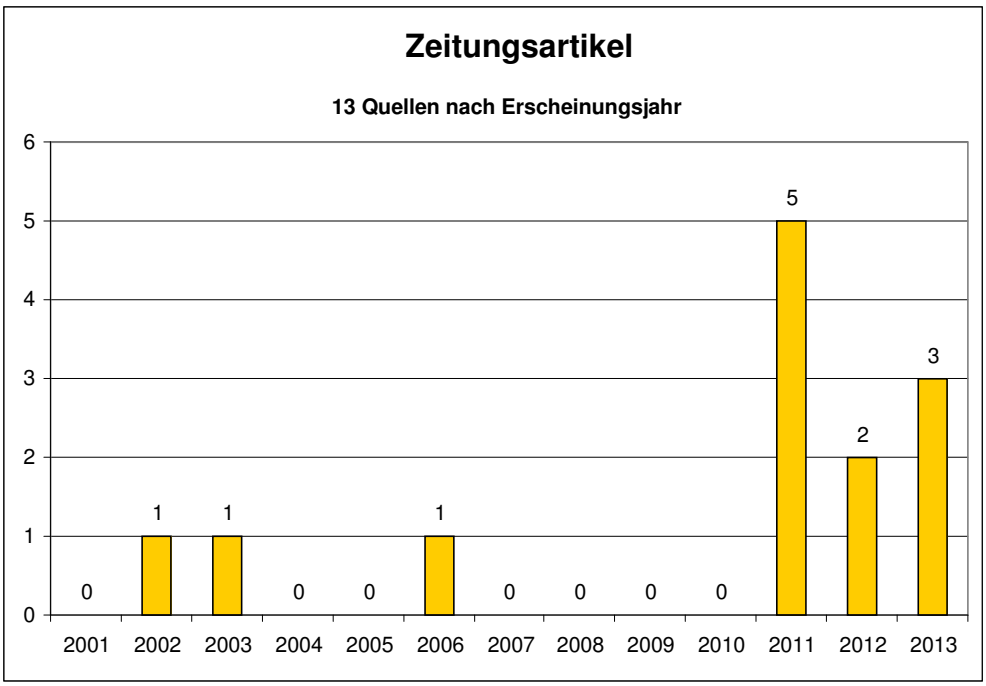

Techniken, Malware, Botnetze
35 Quellen nach Erscheinungsjahr
1 Quelle aus 1994
16
14
12
10
8
6
4
2
0
3
0
0
1
2
2
0
1
1
3
6
14
1
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013


Cyberkriegsführung
6 Quellen nach Erscheinungsjahr
3
2
1
0
0 0 0 0 0 0 1 0 0 0 2 1 2
2001 2002 2003 2004 2005 2006 2007 2008 2009 2010 2011 2012 2013


Insider
5 Quellen nach Erscheinungsjahr
4
3
2
1
0
0 0 0 0 0 0 0 3 0 0 1 0 1
2001 2002 2003 2004 2005 2006 2007 2008 2009 2010 2011 2012 2013


Kultur
4 Quellen nach Erscheinungsjahr
1 Quelle aus 1997
2
1
0
1 0 0 0 0 0 0 1 0 1 0 0 0
2001 2002 2003 2004 2005 2006 2007 2008 2009 2010 2011 2012 2013


Reviews
4 Quellen nach Erscheinungsjahr
2
1
0
0 0 0 1 1 0 0 0 1 1 0 0 0
2001 2002 2003 2004 2005 2006 2007 2008 2009 2010 2011 2012 2013


Zeitungsartikel
13 Quellen nach Erscheinungsjahr
6
5
4
3
2
1
0
0
1
1
0
0
1
0
0
0
0
5
2
3
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013

Anlage 2

Erhebungsbogen für die Akten der Staatsanwaltschaften

Erfassungsbogen Ereignisse StA

lfd. Nummer:

Metadaten

1	Bundesland		
2	Tatzeit	Zeitpunkt des Bekanntwerdens/Tateintritts	
3	TatzeitFrüher	Zeitpunkt eines früheren Tateintritts/Bekanntwerdens	
4	Ort	Ort des Geschädigten/ Tateintritts	
5	Verfahren	Status des Verfahrens zum Zeitpunkt der Abfrage	
6	Verfahrensende		
7	Redundant	unter Polizeiaktenauswertung bereits erfasst	
8	Anhang	anhängige gesonderte Ermittlungsverfahren	
9	Art		

Opfer

10	Geschädigter		
11	Vorschaden	vorher ähnlich geschädigt	

Straftat

12	Straftat1	verletzte Rechtsnorm	
13	Straftat2	(wenn 99 hier selbst zuordnen)	
14	Straftat3		
15	Straftat4		
16	AngrObj	Zielrichtung/ Wirkung der Tat/Angegriffenes Ob	
17	Software	vom Gesch verwendete Software	
18	Vorgehen1	modus operandi	
19	Vorgehen2		
20	Vorgehen3		
21	Vorgehen4		
22	Deface	Sprache und Inhalte Defaces (reiner Text)	
23	Veröffentlichung	Veröffentlichung von Daten (Kundendaten)	
24	Schadenshöhe	finanzieller Schaden	
25	Motiv	in den Akten vermerktes Motiv	
26	VermutMotiv	vermutetes Motiv (Auswerter Projekt)	
27	Deliktsqualität	Bezüge zum Phänomenbereich (in Akten vermerkt)	
28	VermutDelikt	vermuteter Bezug (Auswerter Projekt)	
29	Organisation	Gruppenzugehörigkeit sofern bekannt (z.B. PKK)	
30	international	internationale Bezüge der Tat	

1	1=BW; 2=BY; 3=BR; 4=BB; 5=HB; 6=HH; 7=HE; 8=MV; 9=NI; 10=NW; 11=RP; 12=SL; 13=SN; 14=SA; 15=SH; 16=TH
2	Datum und/oder Uhrzeit
3	0=nein; 1=<6 Monate; 2=<12 Monate; 3=<24 Monate; 4=<36 Monate; 5=ja, aber Tatzeit unbekannt; 99=k.A.
4	Bundesland; Stadt o. ä.
5	1= laufendes Verf.; 2=abgeschlossenes Verf.; 99=k.A.
6	0=laufend; 1=eingst. §170 II StPO; 2=eingst. §153a StPO (Geld); 3=Strafbefehl (CS); 4=Urteil (DS); 99=k.A.
7	0=nein; 1=ja
8	0=nein; 1=ja; 99=k.A.
9	1=öffentl. Interesse; 2=absolutes Antragsdelikt; 3=relatives Antragsdelikt; 99=k.A.

10	1=Privatperson; 2=Schule; 3=Online-Versandhaus; 4=Verein/Kirche; 5=Partei; 6=Produktionsbetrieb; 7=Dienstleistungsunternehmen; 8=Behörden; 9=Medien/Presse; 91=Freiberufler
11	0=nein; 1=einmal; 2=zweimal; 3=über zweimal; 99=k.A. [kurz beschreiben welcher Art]

12	1=202a; 2=202b; 3=202c; 4=303a; 5=303b; 6=263a; 7=269; 8=270 StGB; 9=§ 44 BDSG; 91=130StGB; 92=126 StGB; 93=90b StGB
13	"
14	"
15	"
16	1=Inhalt/Darstellung Webseite; 2=Betrieb einer Webseite; 3=Darstellung und Betrieb einer Webseite; 4=Erreichbarkeit Server; 5=Integrität Datenbestand;
17	1=Joomla; 99=k.A.
18	0=n.b.; 1=Webdefacement; 2=DDoS-Angriff; 3=Ausspähen von Daten; 4=Verändern/Löschen von Daten; 5=Botnetze; 99=k.A.
19	"
20	"
21	"
22	[Inhalte beschreiben, ggf. zitieren]; 99=k.A.
23	0=nein; 1=ja; 99=k.A.
24	in Euro ; 0=nicht zutreffend; 99=k.A.
25	1=Erpressung; 2=Wettbewerbsverhinderung; 3=Übung; 4=Propaganda; 5=Protest; 6=Prahlerei; 99=k.A.
26	0=keine Vermutung; 1=Erpressung; 2=Wettbewerbsverhinderung; 3=Übung; 4=Propaganda; 5=Protest; 6=Prahlerei 99=k.A.
27	1=PMK rechts; 2=PMK links; 3=islamistisch; 4=PMK (z.B. PKK); 5=sonstige; 99=k.A.
28	1=PMK rechts; 2=PMK links; 3=islamistisch; 4=PMK (z.B. PKK); 5=sonstige; 99=k.A.
29	[Freitext]; 99=k.A.
30	0=nein; 1=ja; 99=k.A. [Land/Länder aufschreiben]

Maßnahmen

31	Host	Host Provider	
32	ISP	ISP des Geschädigten bekannt	
33	IP	IP Adresse vorhanden	
34	ErmittIP	Ermittlungsstand anhand IP	
35	ErmittDomain	Abfrage von Bestandsdaten zu Domains/EMailadressen	
36	Proxy	letzter verfolgbarer Angriffs-Server Standort	
37	ErmittInhalt	Ermittlung anhand Inhalten	
38	RechtshiNot	weiterführende Ermittlungsansätze nur mit Rechtshilfeersuchen	
39	RechtsHiErsu		
40	Durchsuchung	Durchsuchungsbeschluss und Durchführung	
41	Asservate	sichergestellte Gegenstände zur Beweissicherung	

Täter

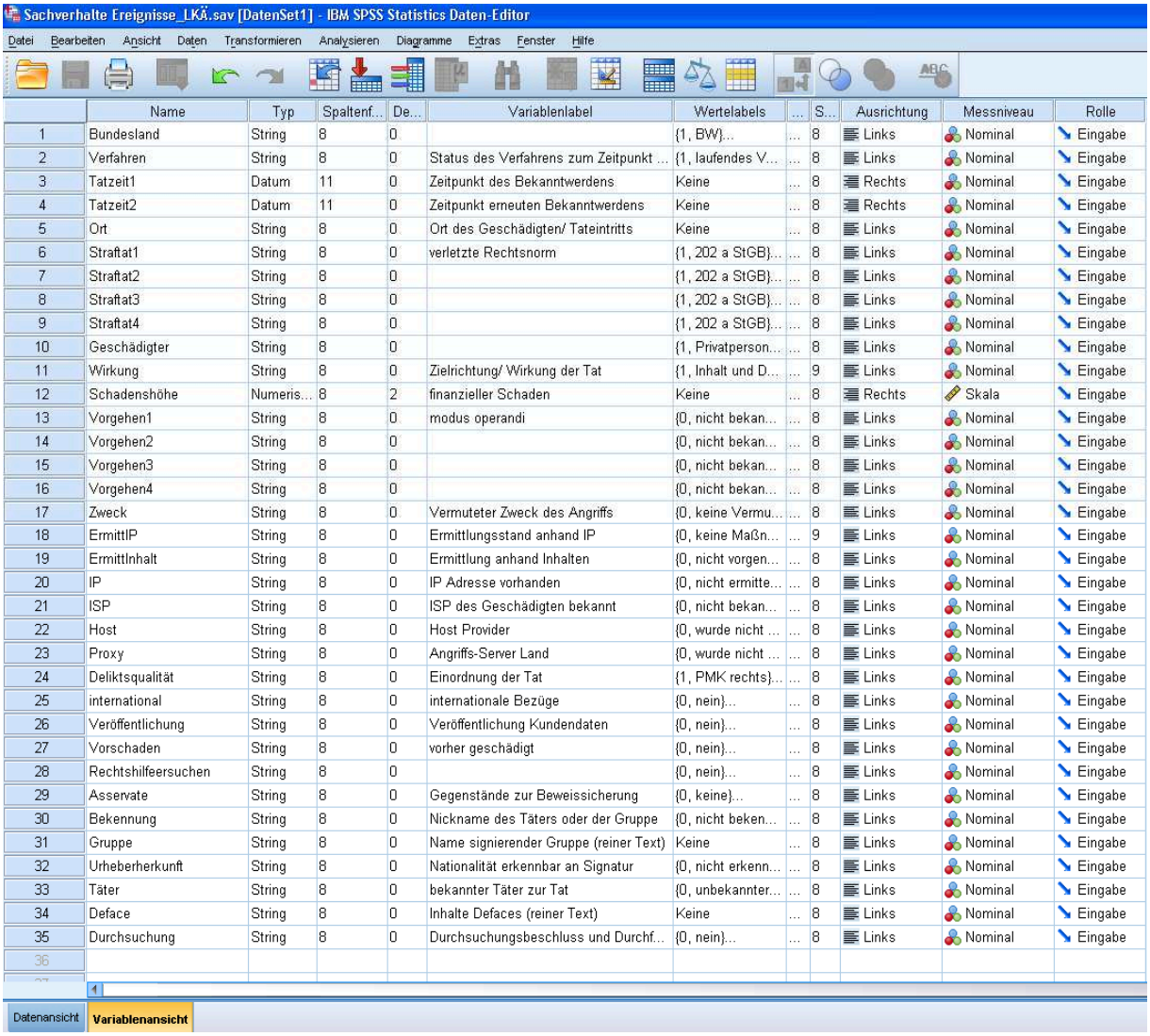
42	Täter	bekannter Täter zur Tat	
43	Bekennung	vom Täter hinterlassene Bekennung zur Tat	
44	Anzahl	Einzeltäter oder Gruppe	
45	Gruppe	Name signierender Gruppe	
46	Urheberherkunft	(vermutete) Staatsangehörigkeit an Signatur/Inhalt erkennbar	
47	ZoneH	Ereignis auf ZoneH.org gelistet	
48	Geschlecht		
49	Altersgruppe		
50	Geburtsort		
51	Familienstand		
52	Staatsangehörigkeit		
53	Hauptwohnsitz		
54	Bildung		
55	Berufsstatus		
56	Vorstrafen		
57	Gruppen		
58	TOA	Täter-Opfer-Ausgleich	
59	Geldstrafe	Gesamtbeträge in Euro	
60	Freiheitsstrafe		
61	AuslStraftat	Täter oder Opfer befinden sich zum Zeitpunkt der Tat im Ausland	
62	Sozialstunden	Numerische Angabe der Stunden	

31	0=nicht kontaktiert; 1=war kooperativ; 2=war unkooperativ; 99=k.A. [ggf. Host-Namen aufschreiben]
32	0=n.b.; 1=bekannt; 99=k.A. [ggf. ISP-Namen aufschreiben]
33	0=nicht ermittelt; 1=bekannt; 2=nicht mehr vorhanden (ISP); 99=k.A.
34	0=k. Maßnahme ergriffen; 1=Anforderung Logfiles; 2=Auswertung Logfiles/Ermittlung Angreifer IP; 3=Provider Ermittlung WhoIs; 4=Anschlussinhaberabfrage beim Provider; 5=IP-Adresse mit Bestandsdaten vorrätig; 99=k.A.
35	0=nicht notwendig; 1=Abfrage erfolgreich (Echtpersonalien); 2=Abfrage erfolglos (fiktive Personalien); 3=nicht vorgenommen; 99=k.A.
36	0=wurde nicht ermittelt; 1=Deutschland; usw. [weiterführen: Land im Freitext eingeben]
37	0=nicht vorgenommen; 1=Open-Source; 2=Polizeiliche Auskunftssysteme; 3=Open-Source/Polizeilich; 4=Auskunftsersuchen an Behörden/ Unternehmen; 5=1und4 zusammen; 6=sonstige [Freitext]; 99=k.A.
38	0=nein; 1=ja; 99=k.A.
39	0=nein; 1=ja, erfolgreich; 2=ja, ohne Erfolg; 3=ja, k. A. zum Erfolg; 99=k.A. [ggf. Land aufschreiben]
40	0=nein; 1=ja; 2= zeitgleiche Durchsuchungen bei OPs; 99=k.A.
41	0=keine; 1=Datenträger; 2=sonstige; 99=k.A. [bei sonstige: kurz benennen]

42	0=unbekannt; 1=Tatverdächtiger; 2=TV Anschlussinhaber; 99=k.A.
43	0=nicht bekennend; 1=bekennend; 99=k.A.
44	0=unbekannt; 1=Einzeltäter; 2=Gruppierung; 99=k.A.
45	[beschreiben bzw. Namen aufschreiben]; 99=k.A.
46	0=nicht erkennbar; 1=Deutschland; 2=Türkei; 3=Gaza; 4=Saudi-Arabien; 5=Palästina; 6=Indien; 7=Russland
47	1=ja; 99=k.A.
48	0=männlich; 1=weiblich
49	0=<14J.; 1=14-18J.; 2=19-23J.; 3=24-28J.; 4=29-33J.; 5=34-38J.; 6=39-43J.; 7=44-48J.; 8=49-53J.; 9=>53J.
50	[Freitext]
51	0=ledig; 1=verheiratet; 2=verwitwet; 99=k.A.
52	0=Deutschland; 1=Türkei; usw. 99=k.A. [anpassen]
53	1=BW; 2=BY; 3=BR; 4=BB; 5=HB; 6=HH; 7=HE; 8=MV; 9=NI; 10=NW; 11=RP; 12=SL; 13=SN; 14=SA; 15=SH; 16=TH
54	0=Schulabbruch; 1=Sonderschule; 2=Hauptschule; 3=Realschule; 4=Gymnasium; 5=FH; 6=Uni; 7=Prom.; 8=sonstiges; 99=k.A.
55	0=erwerbsunfähig; 1=arbeitslos; 2=angestellt; 3=selbstständig; 4=verbeamtet; 5=wehrdienstleistend; 6=Schüler/Student/Ausbildung; 99=k.A.
56	0=nein; 1=Gewalt; 2=Eigentum; 3=BtM; 4=Computer; 99=k.A.
57	0=Einzeltäter; 1=ohne politische Richtung; 2=Anonymous; 3=links, nicht näher bestimmt; 4=rechts, nicht näher bestimmt; 5=islamistisch; 6=PKK; 7=Antifa; 99=k.A.
58	0=nicht geeignet; 1=geeignet; 2=z.Zt. nicht zu bewerten; 99=k.A.
59	[Freitext]
60	[Freitext]
61	0=nein; 1=ja, Opfer; 2=ja, Täter; 99=k.A.
62	Anzahl, 99= k. A.

Anlage 3

Auszug aus der Variablenmaske bei SPSS 21



Sachverhalte Ereignisse_LKÄ.sav [DatenSet1] - IBM SPSS Statistics Daten-Editor

Datei Bearbeiten Ansicht Daten Transformieren Analysieren Diagramme Extras Fenster Hilfe

	Name	Typ	Spaltenf...	De...	Variablenlabel	Wertelabels	...	S...	Ausrichtung	Messniveau	Rolle
1	Bundesland	String	8	0		{1, BW}...	...	8	Links	Nominal	Eingabe
2	Verfahren	String	8	0	Status des Verfahrens zum Zeitpunkt ...	{1, laufendes V...	...	8	Links	Nominal	Eingabe
3	Tatzeit1	Datum	11	0	Zeitpunkt des Bekanntwerdens	Keine	...	8	Rechts	Nominal	Eingabe
4	Tatzeit2	Datum	11	0	Zeitpunkt erneuten Bekanntwerdens	Keine	...	8	Rechts	Nominal	Eingabe
5	Ort	String	8	0	Ort des Geschädigten/ Tateintritts	Keine	...	8	Links	Nominal	Eingabe
6	Straftat1	String	8	0	verletzte Rechtsnorm	{1, 202 a StGB}...	...	8	Links	Nominal	Eingabe
7	Straftat2	String	8	0		{1, 202 a StGB}...	...	8	Links	Nominal	Eingabe
8	Straftat3	String	8	0		{1, 202 a StGB}...	...	8	Links	Nominal	Eingabe
9	Straftat4	String	8	0		{1, 202 a StGB}...	...	8	Links	Nominal	Eingabe
10	Geschädigter	String	8	0		{1, Privatperson...	...	8	Links	Nominal	Eingabe
11	Wirkung	String	8	0	Zielrichtung/ Wirkung der Tat	{1, Inhalt und D...	...	9	Links	Nominal	Eingabe
12	Schadenshöhe	Numeris...	8	2	finanzieller Schaden	Keine	...	8	Rechts	Skala	Eingabe
13	Vorgehen1	String	8	0	modus operandi	{0, nicht bekan...	...	8	Links	Nominal	Eingabe
14	Vorgehen2	String	8	0		{0, nicht bekan...	...	8	Links	Nominal	Eingabe
15	Vorgehen3	String	8	0		{0, nicht bekan...	...	8	Links	Nominal	Eingabe
16	Vorgehen4	String	8	0		{0, nicht bekan...	...	8	Links	Nominal	Eingabe
17	Zweck	String	8	0	Vermuteter Zweck des Angriffs	{0, keine Vermu...	...	8	Links	Nominal	Eingabe
18	ErmittIP	String	8	0	Ermittlungsstand anhand IP	{0, keine Maßn...	...	9	Links	Nominal	Eingabe
19	ErmittInhalt	String	8	0	Ermittlung anhand Inhalten	{0, nicht vorgen...	...	8	Links	Nominal	Eingabe
20	IP	String	8	0	IP Adresse vorhanden	{0, nicht ermitte...	...	8	Links	Nominal	Eingabe
21	ISP	String	8	0	ISP des Geschädigten bekannt	{0, nicht bekan...	...	8	Links	Nominal	Eingabe
22	Host	String	8	0	Host Provider	{0, wurde nicht ...	...	8	Links	Nominal	Eingabe
23	Proxy	String	8	0	Angriffs-Server Land	{0, wurde nicht ...	...	8	Links	Nominal	Eingabe
24	Deliktsqualität	String	8	0	Einordnung der Tat	{1, PMK rechts}...	...	8	Links	Nominal	Eingabe
25	international	String	8	0	internationale Bezüge	{0, nein}...	...	8	Links	Nominal	Eingabe
26	Veröffentlichung	String	8	0	Veröffentlichung Kundendaten	{0, nein}...	...	8	Links	Nominal	Eingabe
27	Vorschaden	String	8	0	vorher geschädigt	{0, nein}...	...	8	Links	Nominal	Eingabe
28	Rechtshilfeersuchen	String	8	0		{0, nein}...	...	8	Links	Nominal	Eingabe
29	Asservate	String	8	0	Gegenstände zur Beweissicherung	{0, keine}...	...	8	Links	Nominal	Eingabe
30	Bekennung	String	8	0	Nickname des Täters oder der Gruppe	{0, nicht beken...	...	8	Links	Nominal	Eingabe
31	Gruppe	String	8	0	Name signierender Gruppe (reiner Text)	Keine	...	8	Links	Nominal	Eingabe
32	Urheberherkunft	String	8	0	Nationalität erkennbar an Signatur	{0, nicht erkenn...	...	8	Links	Nominal	Eingabe
33	Täter	String	8	0	bekannter Täter zur Tat	{0, unbekannter...	...	8	Links	Nominal	Eingabe
34	Deface	String	8	0	Inhalte Defaces (reiner Text)	Keine	...	8	Links	Nominal	Eingabe
35	Durchsuchung	String	8	0	Durchsuchungsbeschluss und Durchf...	{0, nein}...	...	8	Links	Nominal	Eingabe
36											

Datenansicht Variablenansicht