2. Angreifer

Im Anhang A befasst sich das Register vom BSI ausführlich mit den *vorsätzlich handelnden Angreifern im Cyber-Raum*. Die Beschreibungen sind zutreffend und vollständig, bedürfen aber gewisser Ergänzungen, die den Ausprägungen des Hacktivismus und der Cybercrime geschuldet sind.

2.1 Typenlehre von McAfee (2006)

Die erste „Typenlehre“ über die Angreifer im Internet stammt aus McAfee's *Zweiter großer europäischen Studie über das Organisierte Verbrechen und das Internet* vom Dezember 2006 [32].

Die Täter der Internetkriminalität reichen heute (2006) *von Anfängern mit nur eingeschränkten Programmiererkenntnissen, die ihre Angriffe nur mit vorgefertigten Skripts durchführen können, bis hin zu gut ausgebildeten professionell arbeitenden Kriminellen, die über die aktuellen Ressourcen verfügen.*

Nur etwa 2% der *Hacker und Malware-Schreiber* gehören zur puristischen *Elite der Bedrohungsautoren*. Diese ***Innovatoren*** suchen die Herausforderung und nach Sicherheitslücken aus Begeisterung an der Sache. Ihre Gefährlichkeit wird als gering eingestuft, weil sie wissen, was sie tun.

Mittelmäßig gefährlich sind die ***ruhmgierigen Amateure***. Sie sind *Anfänger mit nur eingeschränkten Computer- und Programmiererkenntnissen*, nutzen *vorgefertigte Tools und bekannte Tricks* und suchen nach *Anerkennung in den Medien*. Sie überblicken aber die Folgen ihres Handelns nicht und machen Fehler, die zu ihrer Entdeckung führen.

Gleichermaßen mittelmäßig gefährlich sind die ***Nachahmer***, die Trittbrettfahrer, *die verzweifelt versuchen, ihren berühmten Vorbildern nachzueifern*, aber keine Innovationen oder eigenständige Leistungen in die Szene einbringen.

Beide, die ruhmgierigen Amateure und die Nachahmer, werden heute unter dem abfälligen Begriff ***Skript-Kiddies*** zusammen gefasst.

Aus der Gruppe der *verärgerten oder ehemaligen Mitarbeiter, Zulieferer oder Berater* stammen die hoch gefährlichen ***Insider***. Sie verfügen über Detail- und Exklusivwissen und häufig auch über *Zugangsrechte, die sie während ihrer Mitarbeit erhalten hatten*. McAfee schätzte schon 2006 ihre Bedeutung als steigend ein. Sie handeln böswillig und zielgerichtet, zerstörerisch oder auf ihren finanziellen Vorteil bedacht. Ihnen kann man nur begegnen mit einer klaren, organisatorischen Sicherheitsstruktur und gelebten Sicherheitskultur.

An die Spitze der hoch gefährlichen Kriminellen stellte McAfee die ***Organisierten Internetverbrecher***. *Wie in den meisten Gemeinschaften erfolgreicher Krimineller sitzen tief im Inneren einige streng abgeschirmte Köpfe, die sich auf die Mehrung ihrer Gewinne mit beliebigen Mitteln konzentrieren. Sie umgeben sich mit den menschlichen und technischen Ressourcen, die dies ermöglichen.* Inzwischen wird man sie einerseits nach Koordinatoren [33], Spezialisten, Operation Groups und Rogue-Providern unterscheiden müssen und andererseits nach den besonderen Bedrohungen, die von ihnen ausgehen: Betreiber von Botnetzen [34], Malwarefabriken, Boards [35] und Schurkenprovidern [36].

---

32 *Zweite große europäische Studie über das Organisierte Verbrechen und das Internet*, McAfee Dezember 2006. Leider nicht mehr verfügbar. Auf diese Quelle beziehen sich die unbenannten Zitate in diesem Kapitel. Siehe: **CF**, erste Typenlehre, 27.07.2008.

33 Siehe „Malware-Fabriken“ in Dieter **Kochheim**, IuK-Strafrecht, S. 97.

34 Siehe „Globale Botnetze“ in Dieter **Kochheim**, IuK-Strafrecht, S. 99.

35 Siehe „Boards“ in Dieter **Kochheim**, IuK-Strafrecht, S. 106.

36 Siehe „Schurkenprovider“ in Dieter **Kochheim**, IuK-Strafrecht, S. 100.

2.2 vorsätzlich handelnde Angreifer laut BSI

Das Register unterscheidet zwischen:

▷ Cyber-Aktivisten (Hacktivisten)

▷ Cyber-Kriminelle

▷ Wirtschaftsspione im Cyber-Raum

▷ Staatliche Nachrichtendienste im Cyber-Raum

▷ Staatliche Akteure im Cyber-War (Militär)

▷ Cyber-Terroristen

▷ Skript-Kiddies

Die Beschreibungen sind recht knapp gehalten und werden den Erörterungen in den folgenden Unterabschnitten vorangestellt.

Es ist notwendig, wegen der Cyber-Aktivisten und der Cyber-Kriminellen klarer zu differenzieren. Zwei Gruppen fehlen. Zwischen den staatlichen Nachrichtendiensten und dem Militär fehlen die paramilitärischen Organisationen – McAfee spricht insoweit von „Selbsternannten Internetarmeen, die sich aus anderen Gruppen – vor Allem den Hacktivisten und den Kriminellen rekrutieren – und den Söldnern. Zu denen zähle ich besonders die Unternehmen, die sich spezialisiert haben auf die inhaltliche Auswertung von Datenströmen (Deep Packet Inspection [37]), die Kontrolle und Zensur von Inhalten in Netzen [38], auf Angriffswerkzeuge (zum Beispiel Remote Forensic Software – RFS [39]), Schwachstellen (zum Beispiel Vupen [40]) oder der inhaltlichen Auswertung der Kommunikation in Sozialen Netzen (zum Beispiel HB Gary Federal [41]). Ihre Dienste sind vom Grundsatz her keine Bedrohungen oder gar kriminell, können aber missbraucht werden und das besonders dann, wenn ihr Wissen in falsche Hände gerät.

Einige davon leisten sich den Luxus von öffentlichen Publikationen und Aktivitäten. Dazu zähle ich zum Beispiel McAfee wegen der analytischen Studien [42], GData mit seinen Berichten über Carding-Boards [43], Symantec mit seinen Analysen von Stuxnet [44], Microsoft wegen seiner Maßnahmen gegen das Rustock-Botnetz [45] und jüngst Sophos bei der Enttarnung der Koobface-Gang [46].

Ungenannt bleiben von der BSI auch die Insider, von denen McAfee 2006 gesprochen hat, und die Mitarbeiter, die aus Unwissenheit, Unbedarftheit oder Dummheit Schäden anrichten, aber eben nicht „vorsätzlich“ handeln.

---

37 **CF**, Cyber-Industrieller Komplex, 28.12.2011; David **Talbot**, Das Geschäft mit der Netzüberwachung, Technology Review 23.12.2011

38 Gruselig: Wolfgang **Stieler**, Mein Job beim Big Brother, Technology Review 29.03.2010

39 **CF**, Online-Zugriff an der Quelle, 08.11.2008

40 **CF**, Luigi, das kostet Dich etwas! 14.02.2011

41 **CF**, IT-Söldner im Kampfeinsatz, 15.02.2011

42 **CF**, Studien zur IT-Sicherheit

43 **CF**, neue Hacker-Boards schotten sich ab, 23.05.2010

44 **CF**, Stuxnet doch kein Meisterstück? 15./16.02.1011

45 **CF**, Spam-Schleuder abgeschaltet, 20.03.2011

46 Jan **Drömer**, Dirk **Kollberg**, The Koobface malware gang – exposed! Sophos 17.01.2012

2.2.1 Cyber-Aktivisten (Hacktivisten)

Das sind *Angreifer, die durch einen Cyber-Angriff auf einen politischen, gesellschaftlichen, sozialen, wirtschaftlichen oder technischen Missstand aufmerksam machen oder eine diesbezügliche Forderung durchsetzen wollen ("Hacktivismus"). Die Motivation hinter dem Angriff ist die Einflussnahme. Der durch einen Cyber-Angriff entstandene Schaden wird in Kauf genommen bzw. forciert, um eine höhere Aufmerksamkeit zu erlangen. Sogenannte ethische Hacker fokussieren sich auf gesellschaftliche oder soziale Themen.*

Der Hacktivismus hat eine historische Wurzel in der Hackerbewegung, die vor einigen Jahrzehnten entstand und verschiedenen kulturellen, wirtschaftlichen und zeitgeschichtlichen Einflüssen unterliegt. Es gibt kein einheitliches Bild vom „Hacker“ und dem „Hacktivismus“, zumal sich ganz unterschiedliche Beweggründe und regionale Besonderheiten entwickelt haben. Die Spannbreite reicht von verantwortungsbewussten Gruppen, zu denen ich den deutschen Chaos Computer Club – CCC (1981 gegründet) – zähle, über patriotische, die aus beliebigen Anlässen (zum Beispiel einer Fußballweltmeisterschaft) „gegnerische“ Webseiten verschandeln (Defacement), politische Unterstützer, die in kriegerischen Konflikten wie in Palästina oder Muskelspielen zwischen verschiedenen GUS-Staaten Gegner, Organisationen und Unternehmen angreifen, bis hin zu politischen Protestbewegungen wie Anonymous. Auch die Cyber-Kriminellen haben eine Wurzel im Hacking und nicht zuletzt die Skript-Kiddies, die beide von dem BSI gesondert betrachtet werden.

Auch wenn es den Begriff des „Hacktivismus“ bereits seit 25 Jahren gibt, so ist er mit Nachdruck erst 2010 von Paget in die Diskussion um die Sicherheitsbedrohungen eingeführt worden [47]. Mit der Aktion Payback verschaffte sich seit Herbst 2010 Anonymous eine breite Aufmerksamkeit [48] und in einer aktuellen Studie prognostizieren Paget und andere [49], dass die „weltliche“ Protestbewegung „Occupy“ mit Anonymous verschmelzen wird und dass sich patriotische Bewegungen (nach dem Vorbildern in China) zu selbsternannten und echten Internetarmeen verselbständigen werden.

Die zeitgeschichtliche Brisanz des Hacktivismus gebietet es, auf seine jüngeren Wurzeln und Perspektiven etwas breiter einzugehen.

Die Grundlagen dazu sind bereits beschrieben:

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

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

Dieter **Kochheim**, Eskalationen, 20.02.2011

Dieter **Kochheim**, IuK-Strafrecht, 13.01.2012, S. 20 - 22

47 François **Paget**, Cybercrime and Hacktivism, McAfee Labs 15.03.2010

48 **CF**, kopfloses Kollektiv: Anonymous, 15.02.2011

49 Zheng **Bu**, Toralv **Dirro**, Paula **Greve**, David **Marcus**, François **Paget**, Ryan **Permeh**, Craig **Schmugar**, Jimmy **Shah**, Peter **Szor**, Guilherme **Venere**, Adam **Wosotowsky**, Bedrohungsprognosen für 2012, McAfee Labs 2011

2.2.1.1 Hacker und Hacktivismus

1976 bekam die Hacking-Kultur einen Namen und wurde ihr spezifischer Sprachgebrauch dokumentiert. Das Hacking war mit den Großrechnern in den Sechzigern des letzten Jahrhunderts entstanden und lange Jahre eine sportive akademische Besonderheit. Ihre spielerischen Protagonisten - die Hacker – waren von der Funktionsweise und den Möglichkeiten der IT begeistert, versuchten zu tricksen, fanden Sicherheitslücken und entwickelten bei diesen Gelegenheiten eine besondere Kultur, die zwischen zwei Extremen pendelt: Einerseits geht es ihr um die Absicherung der IT durch das Ausprobieren und Entdecken von Lücken und andererseits wurden mehr und mehr auch profitable Missbräuche praktiziert. Zunächst ging es dabei entweder um den parasitären Zugang zu sehr teurer Rechenzeit oder - mehr und mehr – um den Zugang zu geheimen Informationen anderer. Trotz aller Beteuerungen der "wir sind die Guten" bewegt sich das Hacking noch immer in diesem grauen Spannungsfeld.

Der Begriff „Hacktivism“ geht laut Paget auf 1996 und die Gruppe „Cult of the Dead Cow“ zurück [50]. Diese legendäre Gruppe von Hackern wurde 1984 in Lubbock, Texas gegründet. Ihre Hacktivisten infiltrieren Netzwerke und setzten ihr Können zu Computerangriffen, zur Piraterie, Entführung von Servern und dazu ein, ideologisch geprägte Homepages mit anderen Inhalten zu versehen. Die militanten Hacker wenden sich gegen reaktionäre Meinungsmacher, gegen Scientology, gegen Webseiten der Regierung und gegen große Internet-Unternehmen, denen sie Datenmissbrauch und Geschäftemachereien vorwerfen. Sie blockieren und verunstalten Webseiten, um eine starke Medienaufmerksamkeit zu erregen. Eine bestimmte Nachricht zu verbreiten liefert ihnen häufig nur einen Vorwand für Wettstreite, binnen kürzester Zeit die meisten Webseiten zu verunstalten (Defacement).

Schon immer wurde die Hacker-Bewegung von ruhmgierigen Amateuren und Nachahmern begleitet, wie sie von McAfee 2006 benannt wurden. Für sie hat sich der einheitliche und abfällige Begriff Skript-Kiddies eingebürgert. Er suggeriert, dass es sich um Kinder handelt, die noch Amateure sind, nicht vorhersehen, was sie verursachen, und deshalb nur mit den Mitteln handeln, die sie von anderen bekommen oder abschauen können [51]. Das greift womöglich zu kurz, weil mit dem Erwachsenwerden nicht zwangsläufig verbunden ist, innovativ und vorausschauend zu werden.

Paget hat plastische Beispiele für die frühen Formen der Internetkriminalität vorgestellt. Die organisierten Kriminellen in den USA haben sich danach bevorzugt in den Sparten Glückspiel, Pornographie und Raubkopien betätigt. Im Bereich der GUS-Staaten bestand eine größere Nähe zum Hacking. In Bulgarien und Russland entstanden Viren- und Hacking-Fabriken sowie die Shkola Hackerov ("Hacker-Schulen"), die erste Börse für gestohlene Daten und das nötige Equipment (CarderPlanet) wurde in Odessa gegründet, mit dem Russian Business Network – RBN – entstand in St. Petersburg der erste namhafte Schurkenprovider und in seinem Umfeld wuchsen „innovative“ Entwickler von Mal- und Botware heran. Das zieht sich bis heute fort: 25 Prozent der Absolventen der russischen Wissenschafts- und Technologie-Studiengänge sollen eine Beschäftigung bei einer der beiden im Internet aktiven Mafia-Organisationen finden (Solntsevskaya und Dolgopruadnanskaya). Ende 2011 wurden die Betreiber des Botnetzes DNS Changer in Estland festgenommen [52] und jüngst die Betreiber des Botnetzes Koobface in St. Petersburg identifiziert [53].

---

50 Dieter **Kochheim**, Cybercrime und politisch motiviertes Hacking, 20.10.2010, S. 9;
Grundlage dafür: François **Paget**, Cybercrime and Hacktivism, McAfee Labs 15.03.2010, S. 11, 16.

51 Spannend hat Bongertz nicht nur die Einzelheiten eines erlittenen DoS-Angriffs beschrieben, sondern auch seine Ermittlungen nach dem kindlichen Täter: Jasper **Bongertz**, Nach uns die SYN-Flut, Heise Security 03.08.2011.
Er schließt mit den Worten: *Ich hoffe, der Möchtegern-Blackhat hat richtig Ärger mit seinen Eltern bekommen.*

52 **CF**, Schlag gegen die Organisierte Cybercrime: DNS Changer, 20.11.2011

Es wäre falsch, diese kriminellen Erscheinungsformen mit der Hacker-Bewegung gleichzusetzen. Allenfalls eine gegenseitige Affinität kann darin gesehen werden, dass einzelne prominente Hacker tief in kriminelle Handlungen verwickelt waren und umgekehrt die kriminellen Gruppen auf dieselben Methoden und Mittel zurück greifen, die in der Hacking-Szene entwickelt und verbreitet werden.

2007 erlitt Estland einen groß angelegten DDoS-Angriff, der mehrere Tage lang vor Allem weite Teile staatlicher Präsenzen im Internet lahm legte [54]. In 2008 litten Litauen und Georgien unter Angriffen wegen ihrer Auseinandersetzungen mit Russland. Ein weiterer DDoS-Angriff richtete sich seinerzeit gezielt gegen Radio Free Europe, dessen Programme von den USA gefördert werden.

Über die Identität der Angreifer besteht Unsicherheit und sie werden im regierungsnahen russischen Umfeld vermutet. Eine solche Regierungsnähe vermutet Paget auch wegen der großen Hackergruppen in China (Red Hacker Alliance, China-Eagle-Union, Green Army, Honker Union von China) mit wahrscheinlich mehreren 100.000 Unterstützern.

Die Beispiele zeigen, dass es fließende Übergänge zwischen Hackern, Crackern, Skript-Kiddies und Kriminellen geben muss. Die Hacker-Bewegung als solche gibt es nicht und eine präzise Umgrenzung des Hacktivismus auch nicht. Das führt dazu, dass einzelne Erscheinungsformen wegen ihrer Handlungen, Ziele und Protagonisten genauer betrachtet werden müssen, um ihre Gefährlichkeit und ihr Potenzial zu betrachten.

Ein Beispiel dafür liefert Anonymous.

2.2.1.2 Anonymous und Payback

Drei Organisationen bilden Rahmen für die Bedeutung und neue Qualität, für die das Hacktivismus-Kollektiv Anonymous das Beispiel gibt: WikiLeaks, Anonymous selber und seine spoantaneistischen Randerscheinungen, für die LulzSec steht.

WikiLeaks ist eine Whistleblowing-Plattform, die bereits 2006 entstand und bis 2009 einzelne regimekritische Dokumente aus China und anderen totalitären Staaten veröffentlichte. Seit 2010 erschienen bei WikiLeaks vor Allem USA-kritische Dokumente Schlag auf Schlag:

▷ Video aus der Kamera des Bordgeschützes eines Hubschraubers, das den Beschuss von irakischen Zivilisten und Journalisten zeigt.

▷ Afghanistan-Krieg

▷ Irak-Krieg

▷ diplomatische Depeschen

▷ Guantanamo-Protokolle (April 2011)

Noch keine zivile Organisation hat einen solchen Stepptanz auf den Füßen der USA veranstaltet wie WikiLeaks. Die schnelle Folge und Masse peinlicher und entlarvender Dokumente waren keine Nadelstiche mehr, die mit ein wenig Diplomatie kaschiert werden konnten, sondern schwere Perforationen. Das schrieb ich im Februar 2011 [55].

Schon im März 2008 hatte die CIA gefordert, WikiLeaks zu unterminieren und zu zerstören. Die Kritik an WikiLeaks verschärfte sich 2010. Sie wurde als ein Netzwerk aus Personen und Organisationen bezeichnet, die nur deshalb zusammenarbeiten, um nicht nachverfolgbar massenhaft vertrauliche Dokumente zu veröffentlichen [56]. Dem folgten radikale Handlungsvorschläge [57] und von anderer Seite die Einschätzung [58]: *Wiki-*

53 Jan **Drömer**, Dirk **Kollberg**, The Koobface malware gang – exposed! Sophos 17.01.2012

54 **CF**, DDoS-Angriff auf Estland, 13.07.2008

55 Dieter **Kochheim**, Eskalationen, 20.02.2011, S. 17

56 Palantir Technologies, HBGary Federal, Berico Technologies, The WikiLeaks Threat, 09.02.2011

57 **CF**, Empfehlungen gegen WikiLeaks von Palantir, HBGary Federal und Berico, 15.02.2011

58 Gordon **Bolduan**, "Nur eine Art Aufwärmen". Interview mit John Young, Technology Review

leaks ist eine Geschäftsorganisation, die vorgibt, eine gemeinnützige Organisation zu sein.

Im November 2010 entsann sich Amazon seiner Allgemeinen Geschäftsbedingungen und sperrte den von WikiLeaks gemieteten Hostspeicher. Außerdem erfolgten mehrere DDoS-Angriffe gegen die Plattform mit USA-patriotischem Hintergrund. Die amerikanischen Behörden erwirkten im Dezember 2010 die Sperrung der Domain wikileak.org und mehrere Banken folgten dem Druck und sperrten Konten der Organisation und ihres (nicht immer glücklich agierenden) Sprechers Assange [59].

Die neue Qualität der folgenden zivilgesellschaftlichen Reaktionen zeigte sich in zwei Ereignissen: Weltweit entstanden mehr als Tausend Kopien (Mirrors) von WikiLeaks, so dass die Domainsperre und die DDoS-Angriffe leer liefen. Die Inhalte, gegen die sich die Maßnahmen richteten, waren seither unlöschbar im Internet verankert. Außerdem startete Anonymous die Operation Payback.

Anonymous nennt sich selber das „kopflose Kollektiv“ und besteht aus kleinen stabilen Gruppen und Einzelpersonen [60]. Es trat schon 2008 mit Aktionen gegen Scientology in Erscheinung und 2010 mit DDoS-Angriffen gegen die Organisation der Amerikanischen Filmproduzenten – MPAA – und das indische Unternehmen AiPlex Software [61], um gegen Stilllegung von Pirate Bay zu protestieren. AiPlex führte nach eigenem Bekunden im Auftrag der Filmindustrie Internetangriffe gegen Webseiten mit urheberrechtlich geschützten Filmen durch.

Die Operation Payback richtete DDoS-Angriffe am 07.12.2010 gegen die schweizerische PostFinance, am 08.12.2010 gegen die Kreditkartenunternehmen Visa und Mastercard und am 27.12.2010 gegen die Bank of America.

Mein Kommentar dazu war: *Ein radikaler Teil der Internetgemeinde fordert die Einhaltung von Spielregeln ein! Unternehmen wie Amazon und große Finanzdienstleister können sich nicht mehr wie gewohnt selbstgerecht zurücklehnen, sich auf mehr oder weniger berechtigte AGB-Verstöße berufen, die ihnen so lange nicht aufgefallen sind, wie sie noch in Ruhe Geld verdienen konnten, oder gefahrlos politischem Druck aus dem Mainstream nachgeben. Die Angriffe von Anonymous machen sie zum Angriffsobjekt alternativen Wohlverhaltens. Das ist schmerzhaft!*

Schärfer und mit anderer Ausrichtung formuliert es Messmer [62]: *Kein Staat, kein Unternehmen, keine Rechtsordnung kann akzeptieren, dass ein anarchistischer Schwarm von ein paar Tausend Usern sich auf willkürlich ausgewählte Unternehmen, staatliche und private Organisationen stürzt und deren Webseite – das heißt heutzutage deren Geschäftstätigkeit – für Stunden oder gar Tage lahmlegt.*

2011 trat Anonymous noch mit einigen Operationen auf. Spektakulär war der Hack gegen HB Gary Federal [63] und ins korrekte Bild passen die Einrichtung des Nachrichtenportals Crowdleaks (zunächst: Leakspin) sowie die Unterstützung des Aufstandes in Ägypten. Mit den Angriffen gegen Sony erntete das Kollektiv ernste Kritik – aus der betroffenen Spielerszene [64].

Mit LulzSec tauchte im Frühjahr 2011 eine neue Gruppe auf, die einen beachteten Angriff gegen die Kundendaten bei Sony durchführte und der hohe Professionalität und strategisches Vorgehen nachgesagt wurde [65]. Ihre Aktivisten haben sich auch gleich mit dem FBI angelegt, indem sie dessen Kooperationspartner InfraGard angriffen

---

23.12.2010

59 Siehe: **CF**, Das Ende virtueller (T) Räume, 09.12.2010.

60 Siehe auch: Jan-Keno **Janssen**, Jürgen **Kuri**, Jürgen **Schmidt**, Operation Payback: Proteste per Mausklick, c't 09.12.2010

61 McAfee Threat-Report: Drittes Quartal 2010, McAfee Labs 08.11.2010, S. 23

62 Manfred **Messmer**, Die Zeichen stehen auf Cyberwar, TheEuropean 19.12.2010; siehe auch: **CF**, Streit um den Cyberwar, 05.02.2011.

63 **CF**, IT-Söldner im Kampfeinsatz, 15.02.2011

64 **CF**, Botnetze und Hacktivismus, 08.04.2011

65 **CF**, Sponti-Hacking: LulzSec, 13.06.2011

[66]. Nach 50 Tagen endete die „Überfahrt“ [67], nachdem das „A-Team“, eine gegnerische Gruppe, ein Dossier veröffentlicht hatte, in dem angeblich die wahren Identitäten fast aller LulzSec-Mitglieder aus Großbritannien, Schweden und den USA aufgelistet sind [68].

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

2.2.1.3 Die Zukunft des Hacktivismus

Mit dem Projekt Darknet rief Anonymous im Herbst 2011 auf zur "großen Jagd" gegen die Kinderpornographie und d*ie Glotzer und Nutznießer des Missbrauchs Unschuldiger* [69], deren Daten dabei veröffentlicht werden [70]: Sie zeigen *screen names, manchmal den mutmaßlichen Realnamen, Alter, Geschlecht, dazu bei einigen auch die IP-Adresse, die E-Mail-Adresse, die Postanschrift, den Skypenamen, die Twitteradresse, Homepage und dazu Webadressen von Bildern und einschlägigen Sites, die sie sich angesehen haben, sowie in mehreren Fällen auch die Zugehörigkeit zu Rape-Foren, Fetischseiten, etc.*

Jüngst griff Anonymous das US-Unternehmen Strategic Forecasting – Stratfor – an, das auf internationale Sicherheitsanalysen spezialisiert ist [71]. Rund 4.000 Kundendaten, darunter auch bekannte Unternehmen aus Deutschland, 90.000 Kreditkartendaten und 200 Gigabyte wurden dabei abgegriffen. Diese Aktion und der weihnachtliche Umgang mit den erbeuteten Daten [72] zeigt die Zerbrechlichkeit und Fraktionierung des kopflosen Kollektivs: Es entstand ein offener innerer Streit über den Sinn und die Berechtigung der Aktion.

Die Analysten von McAfee sehen die Entwicklungslinien in der Hacktivismus-Szene als „gemischt“ an [73], *da einzelne Akteure vielfach gegeneinander arbeiteten und oft klare Ziele fehlten. Häufig war es alles andere als einfach, politisch motivierte Kampagnen und die Albernhei-*

66 LulzSec hackt FBI-Liaison und Sicherheitsunternehmen, Heise Security 04.06.2011

67 Der Begriff spielt auf das Wikingerschiff an, das sich LulzSec zum Symbol gemacht hat. Siehe auch: **CF**, Ende der Überfahrt nach 50 Tagen, 28.06.2011.

68 Hackergruppe LulzSec löst sich auf, Heise online 26.06.2011

69 **CF**, Darknet soll Lolita-City unbewohnbar machen, 23.10.2011

70 Thomas **Pany**, Kinderpornografie: Anonymous will Lolita-City unbewohnbar machen, Telepolis 18.10.2011

71 **CF**, Lulzxmas gegen Stratfor, 29.12.2011

72 Sie wurden zu Spenden an gemeinnützige Organisationen missbraucht, die sich dann Rückforderungsansprüchen ausgesetzt sahen.

73 Zheng **Bu**, Toralv **Dirro**, Paula **Greve**, David **Marcus**, François **Paget**, Ryan **Permeh**, Craig **Schmugar**, Jimmy **Shah**, Peter **Szor**, Guilherme **Venere**, Adam **Wosotowsky**, Bedrohungsprognosen für 2012, McAfee Labs 2011.
Alle folgenden Verweise betreffen die S. 4 – 5.

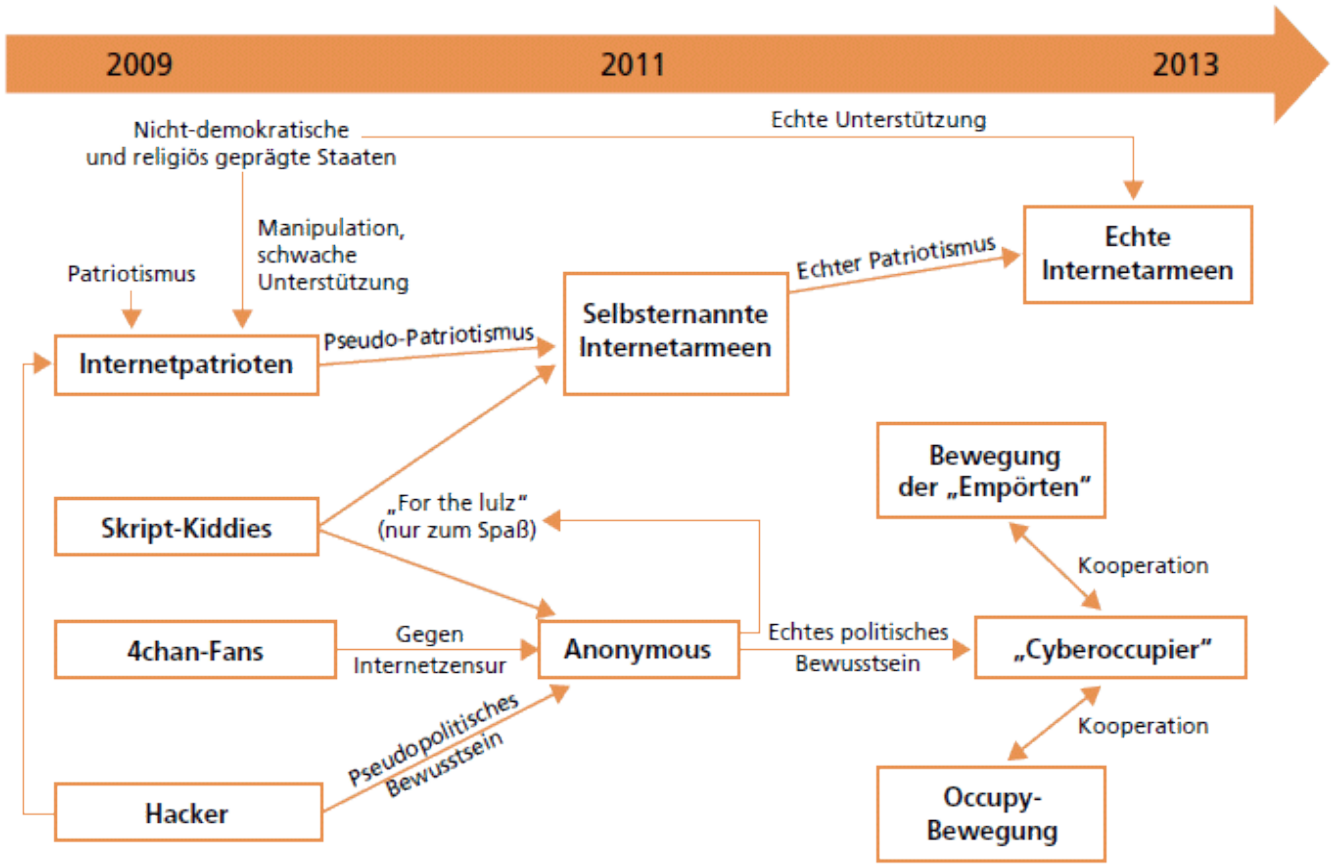

Abbildung 1. Die verschiedenen Verbindungen und Motivationen von Hacktivismus.

ten von Skript-Kiddies auseinander zu halten. Eines wurde jedoch schnell klar: Wenn Hacktivisten ein Ziel auswählten, wurde es durch einen Dateneinbruch oder eine Denial-of-Service-Attacke kompromittiert. Deshalb sollten diese Gruppierungen ernstgenommen werden. Ganz gleich, ob man mit ihren Zielen einverstanden ist oder nicht, Anonymous und andere Hacktivisten-Gruppen haben sich bei der Wahl ihrer Ziele und Vorgehensweisen als zielstrebig, einfallsreich und flexibel erwiesen.

Aus ihrem Bericht stammt die oben abgebildete Grafik, die sich sehr gut in eine obere und eine untere Hälfte teilen lässt [74].

In die Anonymous-Bewegung sehen sie Hacker, Skript-Kiddies und „4chan-Fans" einfließen, wobei es sich um die Nutzer des Imageboards 4chan.org handelt, das für die ungehemmte (freie) Verbreitung in aller Regel unbedachter Kommentare und Grafiken bekannt ist. Aus Anonymous und der (weltlichen) Occupy-Bewegung sieht McAfee die „Cyberoccupier" entstehen, wenn Anonymous es schafft, *konzertierte und verantwortungsbewusste* Aktionen durchzuführen. Sonst droht die Marginalisierung (Verelendung, Verdrängung).

Sollte die Verbindung gelingen, dann könnte sich daraus tatsächlich eine schlagkräftige zivilgesellschaftliche Bewegung entwickeln, die sehr gezielt bürgerlichen Ungehorsam, klassische Protestaktionen und internettypische Angriffe kombiniert.

Auf das Internet bezogen prognostiziert McAfee eine Zunahme politisch motivierter DDoS-Angriffe und Kompromittierungen persönlicher Daten. Auch ungeachtet der Cyberoccupier wird eine stärkere Vernetzung zwischen physischen Protesten und dem Hacktivismus unter Nutzung der Sozialen Netze und Medien erwartet, wobei die „realen" Protestbewegungen ihre Aktionen zunehmend mit virtuellen Angriffen kombinieren werden [75]. Nicht nur Hacking-Angriffe werden da-

74 Den einzigen Verbindungspunkt stellen die Skript-Kiddies dar, denen organisatorisches Talent, Weitsicht oder Führungsstärke eher nicht nachgesagt wird.

75 Auch das ist nicht neu: Schon Ende 2010 wurde die Berliner Hausbesetzerszene von Aktionen

nach zunehmend individueller werden, sondern auch die politisch motivierten Aktionen: *Aus politischen und ideologischen Gründen wird das Privatleben öffentlicher Personen wie Politiker, Unternehmensführer, Richter sowie Strafverfolger und Sicherheitsbeamter im neuen Jahr öfter als bisher öffentlich gemacht. Die Protestierenden werden sich kaum aufhalten lassen, wenn es darum geht, Daten von sozialen Netzwerken oder Web-Servern zu erlangen, um ihre unterschiedlichen Aktionen zu unterstützen.*

2.2.1.4 Fazit: Zukunft des Hacktivismus

Ich glaube nicht, dass die Occupy-Bewegung erst auf ein verlässliches kopfloses Kollektiv warten muss, sondern dass zwischen Occupy und Annonymous bereits so viele Querverbindungen bestehen, dass sie sich längst gegenseitig fördern, befruchten und beeinflussen. In seinen Ursprüngen war Anonymous eine „reale“ Protestbewegung, die sich bei den Aktionen durch ihre Guy Fawkes-Masken ausgezeichnet hat.

McAfee beschreibt – überraschend wohlwollend – ein allgemeines Problem von Protestbewegungen, denen klare Ziele und etwas charismatische Führung fehlen: Sie zerfasern und zerfallen leicht aufgrund interner Rivalitäten, Richtungsstreite und bröckelnder Motivation. Auch „klare Ziele“ haben ihre Nachteile. Sie führen schnell zu religiös anmutenden Dogmen und verkrusteten Herrschaftsstrukturen.

Occupy und Anonymous haben die wichtige Funktion, dass sie die Forderungen nach bürgerlichen Freiheiten besetzen. Ob sie bei der gesellschaftlichen und wirtschaftlichen Analyse, bei der Auswahl ihrer Angriffsziele und bei der Durchführung ihrer Aktionen immer richtig liegen und Augenmaß beweisen, ist eine andere Frage. Das gilt besonders dann, wenn es um die Rechte anderer und den Ausgleich verschiedener Anforderungen geht.

Anonymous und LulzSec haben gezeigt, dass dort erfahrene (und erwachsene) Leute aktiv werden, die über hochgradiges Wissen und praktische Erfahrung verfügen, um kleine oder große politische Ziele mit Hacking-Methoden zu fördern und zu erreichen. Sie müssen sich hinter abgebrühten IT-Profis und Kriminellen nicht verstecken.

Sie sind wahrscheinlich geprägt von der Open Source-Bewegung. Das heißt nicht, dass sie freie Software schreiben, sondern dass sie so etabliert sind, dass sie sich hacktivistische Freizeitaktivitäten leisten können, ohne auf das eigene Einkommen zu achten. Das unterscheidet sie maßgeblich von den Cyber-Kriminellen und den IT-Söldnern.

---

begleitet, bei denen Webshops verschandelt wurden (Defacement): **CF**, Molotowcocktails im Internet, 05.02.2011.

Für die Skript-Kiddies müsste man eine eigene Welpenschutzorganisation gründen. Wenn sie schon nicht richtig programmieren können und auch nicht wissen, was sie anrichten, dann kann ihnen auch keine politische Weitsicht abverlangt werden.

Was wird aus ihnen, wenn sie zwangsläufig heranwachsend und erwachsen werden? Die ersten Erfahrungen aus den Carding-Boards zeigen mir, dass sie immer abgebrühter und dissozialer werden, nicht aber Gewissen und innovative Kreativität entwickeln, wenn es darum geht, die IT-Sicherheit und damit das Gemeinwohl zu fördern.