Bundeskriminalamt

HACKTIVISTEN

Hacking + Aktivismus

=

Hacktivismus

Zusammenfassung

Bundeskriminalamt
Kriminalistisches Institut
Forschungs- und Beratungsstelle Cybercrime IZ36
iz36@bka.bund.de

BKA

Zusammenfassung

Das Projekt wurde mit dem Ziel initiiert, die Erkenntnisse zum Cybercrime-Phänomen Hacktivismus zu erweitern und auf eine fundierte Wissensbasis zu stellen.

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. Empirisch wurde die Erkenntnisbasis durch die Analyse registrierter hacktivistischer Fälle in Deutschland sowie durch die Befragung von Unternehmen und öffentlichen Einrichtungen in Deutschland erweitert und fundiert. Die Zahl der ausgewerteten Fälle (78 bereinigt[1] bzw. 183 insgesamt) und Befragungsdaten (971) erlaubt generalisierbare Aussagen sowohl zu deutschen polizeibekannten Fällen als auch zu hacktivistischen Fällen, die bislang im Dunkelfeld verblieben.

Mittels Sekundär- und Fallanalyse, Medienrecherche und Online-Befragung konnten Aussagen zu Vorgehensweisen, Verschleierungstechniken und in geringerem Umfang auch zur Kommunikation gewonnen werden. Auch Entwicklungen und Szenedynamiken konnten beschrieben werden. Aussagen zu Schäden ließen sich nur beispielhaft gewinnen und zusammentragen, die Repräsentativität der Schadensangaben in den Fallakten ist nicht gewährleistet. Die Repräsentativität der Aussagen zu Schäden durch Hacktivismus in den IT-Sicherheitsberichten kann aufgrund mangelnder Transparenz der Methodik nicht bewertet werden. Die Datenlage sowohl der Auswertungen mittels Sekundäranalyse und Fallanalyse als auch mittels Medienrecherche 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.

[1] 106 Fälle stammen aus einem Verfahren und wurden für viele Berechnungen (wie z. B. modi operandi) als ein Fall gezählt.

wie stark diese Erkenntnisse durch Merkmale von Gelegenheits-Sympathisanten und/oder Mitläufern geprägt sind.

Hacktivismus zeichnet sich insbesondere durch eine nicht-profitorientiere und ideologisch motivierte Ausübung von Taten zum Zwecke des Protests und der Propaganda aus und wird überwiegend von Gruppierungen ausgeübt. Diese Gruppierungen haben keine feste Mitgliederzahl, weisen (bis auf wenige Ausnahmen wie z. B. Lulzsec) keine Hierarchie und keine Kontrolle auf und üben häufig auch Aktivitäten ohne hacktivistische Ausrichtung aus (wie z. B. bloßes Hacking oder „Spaßaktionen“ wie bei Anonymous). Einzeltäter sind eher selten, da sich politisches und soziales Engagement in Gruppen ausdrückt. Die Mehrheit (ca. 90 %) der hacktivistisch agierenden Personen sind männlich und zwischen 16 und 30 Jahre alt.

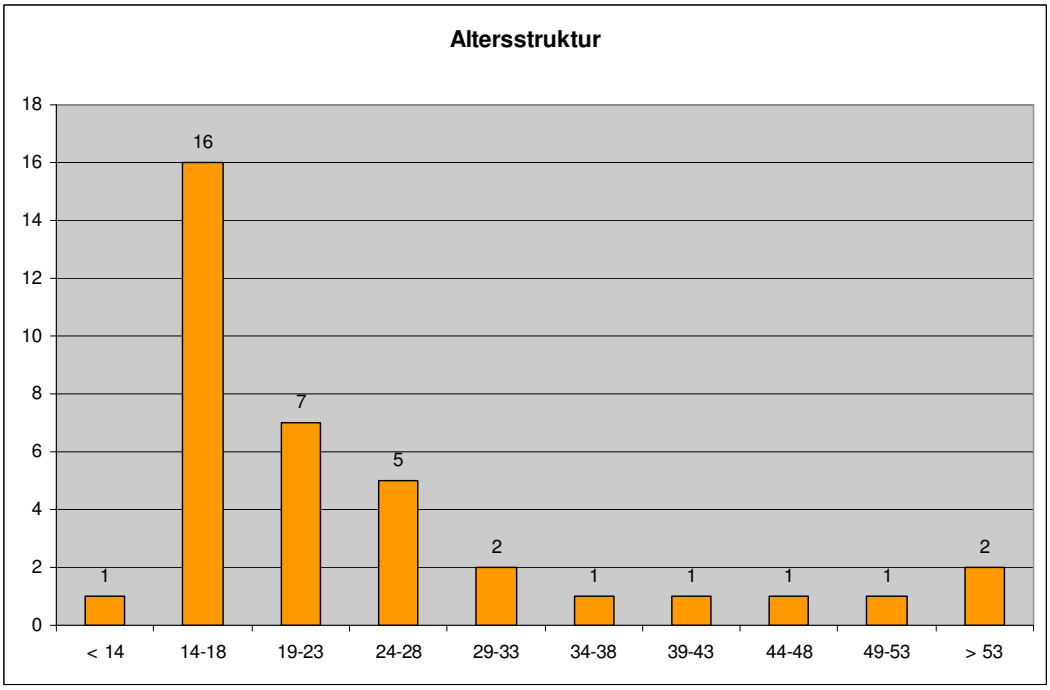

Abbildung 1: Altersverteilung bei 37 Beschuldigten (Fallanalyse)

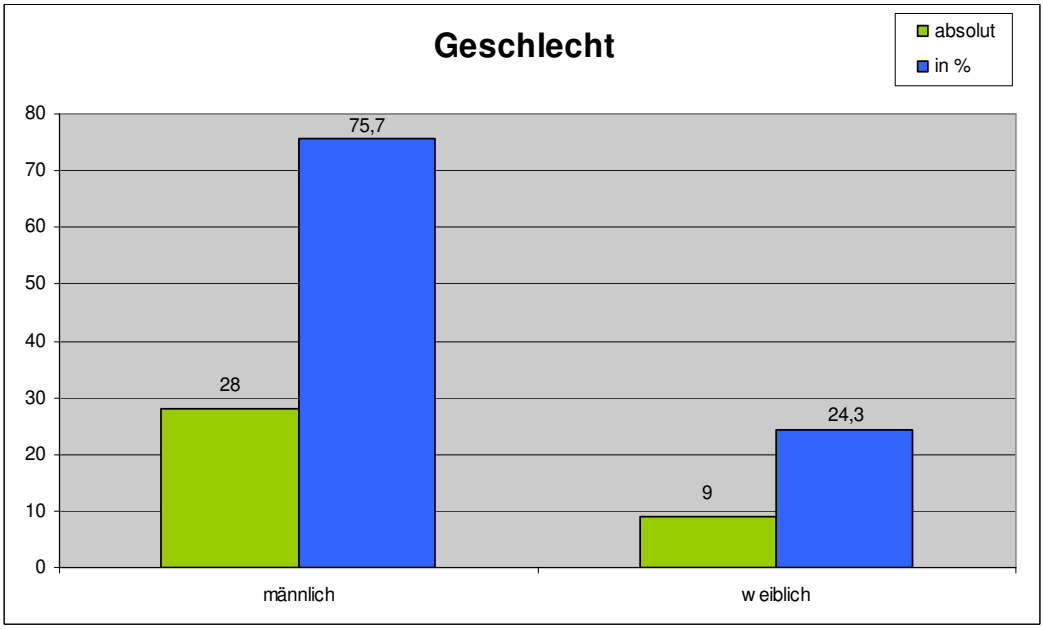

Abbildung 2: Geschlechterverteilung bei 37 Beschuldigten (Fallanalyse)

Belastbare Erkenntnisse zu sozioökonomischen Merkmalen liegen derzeit nicht vor. Aus der Fallanalyse ergibt sich der Hinweis auf eine Mehrheit an Schülern, Studenten und Auszubildenden, was auch der vorherrschenden Altersgruppe der Hacktivisten entsprechen würde. Bevorzugte Vorgehensweisen der Hacktivisten sind Web-Defacement, DDoS-Angriffe sowie das Ausspähen und Manipulieren von Daten. Geschädigte von Hacktivismus sind in erster Linie Regierungen (und Angehörige) und Unternehmen, wobei – dem Anzeigeverhalten von Unternehmen geschuldet – in der Fallanalyse Privatpersonen die Mehrheit der Geschädigten ausmachen.

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

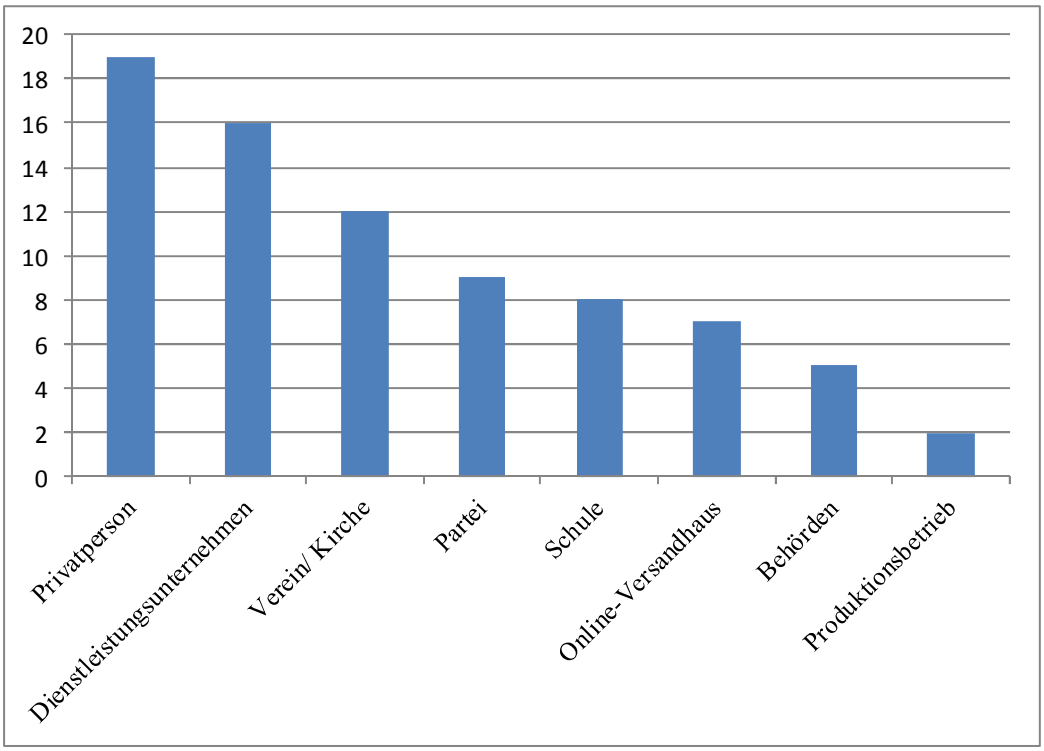

Abbildung 4: Geschädigte in 78 Fällen (Fallanalyse)

Von 971 Unternehmen, die an der Online-Befragung teilnahmen, gaben 80 Unternehmen an, bereits ein- oder mehrmals von Hacktivismus betroffen gewesen zu sein. Damit liegt die Häufigkeit für Unternehmen und öffentliche Einrichtungen in Deutschland Ziel von Hacktivismus zu werden bei 8 %. Hier sind es insbesondere Unternehmen aus der Branche Information und Kommunikation, die überdurchschnittlich häufig mit hacktivistischen Angriffen belastet sind.

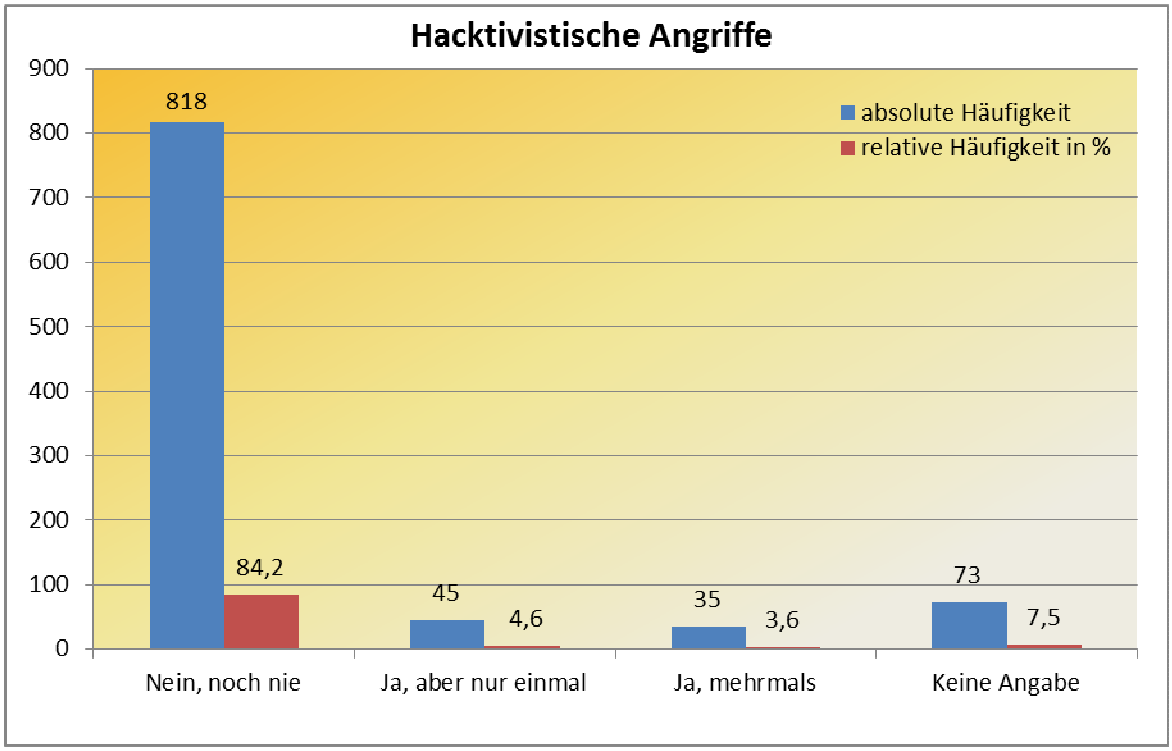

Abbildung 5: Hacktivistische Angriffe auf Unternehmen und öffentliche Einrichtungen (Online-Befragung)

Die Unternehmensgröße spielt hinsichtlich der Angriffshäufigkeit eine Rolle: Je größer das Unternehmen ist, desto eher war es bereits mehrmals von hacktivistischen Angriffen betroffen. 60 % der betroffenen Einrichtungen behoben die Schäden intern, 15 % erstatteten Anzeige. Als Gründe, von einer Anzeigenerstattung abzusehen, gaben 33 % der Unternehmen an, dass es keine Angriffsfolgen gab, auch wenn ein folgenloser Angriff strafbar sein kann. 40 % sahen in einer Anzeigenerstattung keine Aussicht auf Erfolg. Für das Dunkelfeld von Hacktivismus bedeuten diese Ergebnisse, dass die Anzeigequote für hacktivistische Aktivitäten bei 15 % liegt und damit 85 % der

Aktivitäten im relativen Dunkelfeld liegen (68 Fälle). Dem Dunkelfeld hinzuzurechnen sind die Fälle, welche vom Opfern nicht bemerkt werden (absolutes Dunkelfeld).

Insgesamt konnte im Rahmen der Medienrecherche bestätigt werden, dass das Thema Hacktivismus auch im Darknet eine Rolle spielt: Im Forum „Deutschland im Deep Web“ wurde die Diskussion zur Gründung einer neuen hacktivistischen Gruppierung mitverfolgt, deren Ausgang jedoch offen blieb. Auch die Seiten „Hack the Planet“ und „CODE GREEN“ thematisieren den Hacktivismus. Einen eindeutigen Bezug zu Deutschland wies jedoch nur das Forum „Deutschland im Deep Web“ auf.

Die Bewertung von Gefährdungs- und Schadenspotenzial von Cybercrime-Phänomen ist insbesondere abhängig vom Zielobjekt und der vom Täter genutzten Vorgehensweise. Auch wenn das Gefährdungs- und Schadenspotenzial für Hacktivismus derzeit als gering anzusehen ist, zeichnet sich ab, dass Hacktivismus zunehmend in Form von „combined attacks“ stattfinden wird, 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.[2] Unternehmen bzw. Einrichtungen, die social media einsetzen, sollten auch eine entsprechende Kompetenz im Umgang mit auftretenden Konflikten vorweisen, damit solche Situationen nicht in hacktivistischen Angriffen münden.
Es 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

[2] Dies zeichnet sich bereits bei Shitstorms ab, aus denen sich Verabredungen zu Angriffen hacktivistischer Natur ergeben können.

ausgeschlossen sind. Um an einer derartigen „Demo“ teilzunehmen, genügt ein einfacher Mausklick. Den meisten Nutzern ist in dem Moment allerdings nicht klar, dass sie mit dem damit ausgelösten DDoS-Angriff eine Straftat begehen. Die Risikowahrnehmung und die Medienkompetenz der Bürger und Internetnutzer muss dahingehend ausgeprägt werden, dass klar wird, welche Taten im Internet strafbar sind.

Die Ergebnisse sowohl der Sekundär- und Fallanalyse als auch der Medienrecherche und Online-Befragung lieferten weder im Hellfeld noch im Dunkelfeld Belege für ein signifikantes Bedrohungspotenzial durch hacktivistische Taten. Auf Grundlage der Zahlen zu Schäden, lässt sich derzeit kein hohes Schadenspotenzial durch Hacktivismus ausmachen, zumindest was Angriffe auf Geschädigte in Deutschland betrifft. Es ist zu vermuten, dass bei entsprechender Organisation und Kommunikation zur Sympathisantengewinnung hacktivistische Aktionen und Angriffe in der Zukunft nicht abnehmen werden, sondern eher zunehmen.

Abbildungsverzeichnis

Abbildung 1: Altersverteilung bei 37 Beschuldigten (Fallanalyse) *2*
Abbildung 2: Geschlechterverteilung bei 37 Beschuldigten (Fallanalyse) *3*
Abbildung 3: Hacktivistische Zielrichtungen. (Held, W.V. (2012). Hacktivism: an Analysis of the Motive to Disseminate Confidential Information) *4*
Abbildung 4: Geschädigte in 78 Fällen (Fallanalyse) *4*
Abbildung 5: Hacktivistische Angriffe auf Unternehmen und öffentliche Einrichtungen (Online-Befragung) *5*

Literatur des Abschlussberichts

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

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

Harm, R. *ONLINE-DEMONSTRATIONEN. Best-Practices für die Mobilisierungsarbeit*
im Netz. http://manuals.sozialebewegungen.org/onlinedemos/

Heckmann, D. (2014). *jurisPK-Internetrecht*. Kap. 8. juris

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

Hilgendorf, E./Wolf, Chr. (2006). *Internetstrafrecht - Grundlagen und aktuelle Fragestellungen*. K&R 2006, 541-547

Hoffmanns, S. (2012). *Die "Lufthansa-Blockade" 2001 - eine (strafbare) Online-Demonstration?* ZIS 2012, 409-414

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

Kappler, M./ Nicklas, F. (2012). *Blitzkrieg im Internet.* http://www.vice.com/de/read/blitzkrieg-anonymous-npd-nazis (Stand: 17.06.14).

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

Kumar, M. (2011). *National Democratic Party (NPD) of Germany hacked by n0-N4m3 Cr3w.*
http://thehackernews.com/2011/06/national-democratic-party-npd-of.html (27.06.14).

Leyden, J. (2009). *German Interior minister's website pwned in wiretap protest.*
http://www.theregister.co.uk/2009/02/11/german_minister_website_hack/ (Stand: 27.06.14).

Libbenga, J. (2005). *Lufthansa online activist found guilty.*
http://www.theregister.co.uk/2005/07/05/lufthansa_demo/ (Stand: 27.06.14).

März, A. (2010.) *Mobilisieren: Partizipation – vom ‚klassischen Aktivismus' zum Cyberprotest.* in: Baringhorst, S. et al. (2010.) *Unternehmenskritische Kampagnen. Politischer Protest im Zeichen digitaler Kommunikation.* Springer-Verlag

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

Möhlen, Chr. (2013). *Das Recht auf Versammlungsfreiheit im Internet – Anwendbarkeit eines klassischen Menschenrechts auf neue digitale Kommunikations- und Protestformen*. In: MultiMedia und Recht Heft 4/2013. S. 221-229

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

Pötters, S./Werkmeister, C. (2011). *Neue Problemkreise des Versammlungsrechts: Konturierung des Schutzbereichs des Art. 8 Abs. 1 GG.* http://www.zjs-online.com/dat/artikel/2011_3_449.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

Redi, A./ Kovacs, E. (2013). *Softpedia Interview: Alberto Redi, Head of Zone-H.* http://news.softpedia.com/news/Softpedia-Interview-Alberto-Redi-Head-of-Zone-H-359499.shtml

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

Thiele, A. (2009). *Basiswissen Staatsrecht II – Grundrechte*. Niederle Media

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

Anhang

Liste der gesichteten IT-Sicherheitsberichte

	Titel	Daten aus dem Jahr	Unternehmen/ Institution	DDos	Data Breach	Defacement	Zahlen zu Kosten	Hacktivismus als eigene Kategorie	Daten zu Deutschland
	2013 Cost of Cyber Crime Study: Global Report	2013	Ponemon Institute (Sponsored by HP Enterprise Security)	✓	o	x	✓	x	o
	2013 Cost of Cyber Crime Study: Germany	2013	Ponemon Institute (Sponsored by HP Enterprise Security)	✓	o	x	✓	x	✓
	2013 Cost of Cyber Crime Study: United States	2013	Ponemon Institute (Sponsored by HP Enterprise Security)	✓	o	x	✓	x	x
	2012 Cost of Cyber Crime Study: Germany	2012	Ponemon Institute (Sponsored by HP Enterprise Security)	✓	o	x	✓	x	✓
	2012 Cost of Cyber Crime Study: United States	2012	Ponemon Institute (Sponsored by HP Enterprise Security)	✓	o	x	✓	x	x
	2014 Cost of Data Breach Study: Global Analysis	2013	Ponemon Institute (Sponsored by IBM)	x	✓	x	✓	x	o
	2013 Cost of Data Breach Study: Global Analysis	2012	Ponemon Institute (Sponsored by Symantec)	x	✓	x	✓	x	o
	2014 Cost of Data Breach Study: Germany	2013	Ponemon Institute (Sponsored by IBM)	x	✓	x	✓	x	✓
	2013 Cost of Data Breach Study: Germany	2012	Ponemon Institute (Sponsored by Symantec)	x	✓	x	✓	x	✓
	2013 Cost of Data Center Outages	2013	Ponemon Institute (Sponsored by Emerson Network Power)	o	x	x	✓	x	x
	2013 Annual Cost of Failed Trust Report: Threats & Attacks	?	Ponemon Institute (Sponsored by Venafi)	x	o	x	✓	x	✓
	2012 Data Breach Investigation Report	2011	Verizon Communications Inc.	x	✓	x	x	o	x
	2013 Data Breach Investigation Report	2012	Verizon Communications Inc.	o	✓	x	x	o	x
	2014 Data Breach Investigation Report	2013	Verizon Communications Inc.	o	✓	x	x	o	x
	2014 The Danger Deepens - Neustar Annual DDoS Attacks and Impact Report	2013	NeuStar, Inc.	✓	x	x	✓	x	x
	Hope Is Not a Strategy- 2012 Annual DDoS Attack and Impact Survey: A Year-to-Year Analysis	2012	NeuStar, Inc.	✓	x	x	✓	x	x
	Worldwide Infrastructure Security Report, Volume IX	2013	Arbor Networks, Inc.	✓	x	x	x	x	x
	Worldwide Infrastructure Security Report, Volume VII	2012	Arbor Networks, Inc.	✓	o	x	x	x	x
	The Economic Impact of Cybercrime and Cyber Espionage	2013???	McAfee	x	o	x	✓	x	x
	Net Losses: Estimating the Global Cost of Cybercrime (Economic Impact of Cybercrime and Cyber Espionage II)	2014??	McAfee	x	o	x	✓	x	x
	Internet Security Threat Report 2013	2012	Symantec	o	✓	x	x	o	x
	Internet Security Threat Report 2014	2013	Symantec	o	✓	x	x	o	x
	2012 Internet Crime Report	2012	FBI	x	x	x	✓	x	x
	2013 Internet Crime Report	2013	FBI	x	x	x	✓	x	x
	Kaspersky Security Bulletin: 2013/2014	2013	Kaspersky	o	✓	x	o	o	x
Summe	25			9	10	0	17	0	5

Anmerkung: Die Tabelle zeigt welche Auswahlkriterien von den 25 gesichteten Berichten erfüllt werden: ✓ = erfüllt; x = nicht erfüllt; o = teilweise erfüllt.