Bundeskriminalamt

HACKTIVISTS

Hacking + Activism

=

Hacktivism

Summary

Bundeskriminalamt
Kriminalistisches Institut
Forschungs- und Beratungsstelle Cybercrime KI 16
ki16@bka.bund.de

The project was initiated with a view to expanding information on the cybercrime phenomenon of hacktivism and to placing it on a sound knowledge base.

As a result, the project has provided a clear differentiation between the concept of hacktivism and those of related and similar tendencies in this area of crime as well as a sound information basis regarding the hacktivism phenomenon. Empirically, the information basis was expanded and consolidated by an analysis of the cases of hacktivism registered in Germany and a survey of companies and public institutions in Germany. The number of cases analysed (78 after adjustment [1], 183 in total) and survey data gleaned from online questionnaires (971) allows generalisable statements to be made about German cases which are known to the police as well as cases of hacktivism that have gone unreported and unrecorded thus far.

Information about modi operandi, cover-up methods and, to a lesser extent, communication was obtained by means of secondary and case analysis, media research and an online survey. It was also possible to describe developments and dynamics within the scene. Information obtained and compiled about losses caused was only exemplary; it is not possible to ensure that information about damages in the case files is representative. The representativeness of the information in the IT security reports about damages caused by hacktivism cannot be assessed due to lack of transparency of the methods employed. It was not possible to identify typologies on the basis of data obtained by secondary and case analysis as well as media research. It was only possible to make statements about hacktivist offenders of registered crimes. The generalisability of such information is, however, extremely limited due to a variety of factors: The offenders, who were subject to case analysis, were merely involved in a hacktivist attack, which means it is uncertain how many of the suspects were only hangers-on. Neither does information obtained via secondary analysis reveal whether it refers to actual hacktivists in terms of ideologically motivated persons, i.e. activists, or whether it is strongly influenced by characteristics of occasional sympathisers and/or hangers-on.

Hacktivism is particularly characterised by a non-profit-oriented and ideologically motivated commission of offences for protest and propaganda purposes and is mainly

[1] 106 cases belong to one specific investigation and were regarded as one single case for many calculations (such as modi operandi).

carried out by groups. These groups do not have a fixed number of members, a hierarchical structure or control mechanisms (although there are a few exceptions, such as "Lulzsec") and frequently also engage in activities which do not have a hacktivist orientation (such as mere hacking or pranks as in the case of "Anonymous"). Lone offenders are rather rare, since political and social commitment is mostly expressed in groups. The majority (approx. 90%) of persons conducting hacktivist activities is male and between 16 and 30 years old.

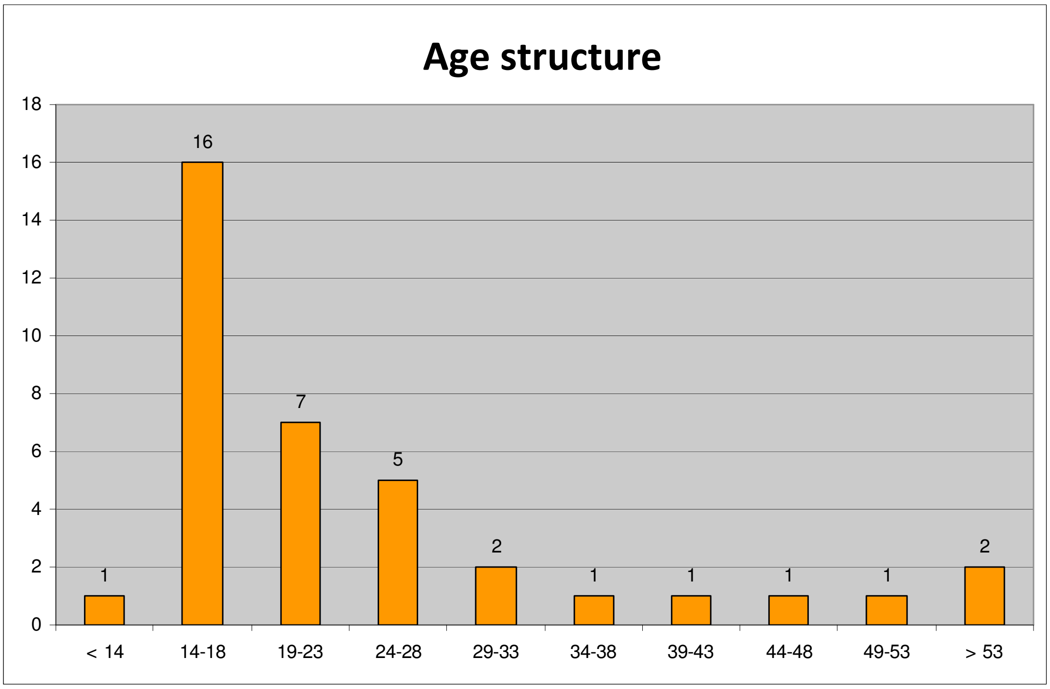


Figure 1: Age distribution among 37 suspects (case analysis)

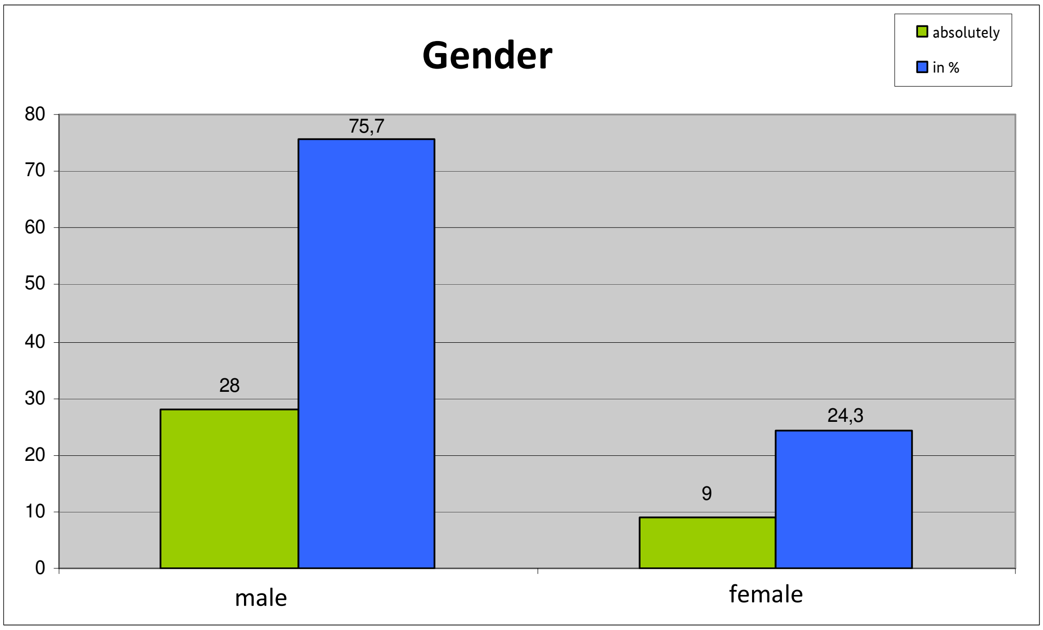
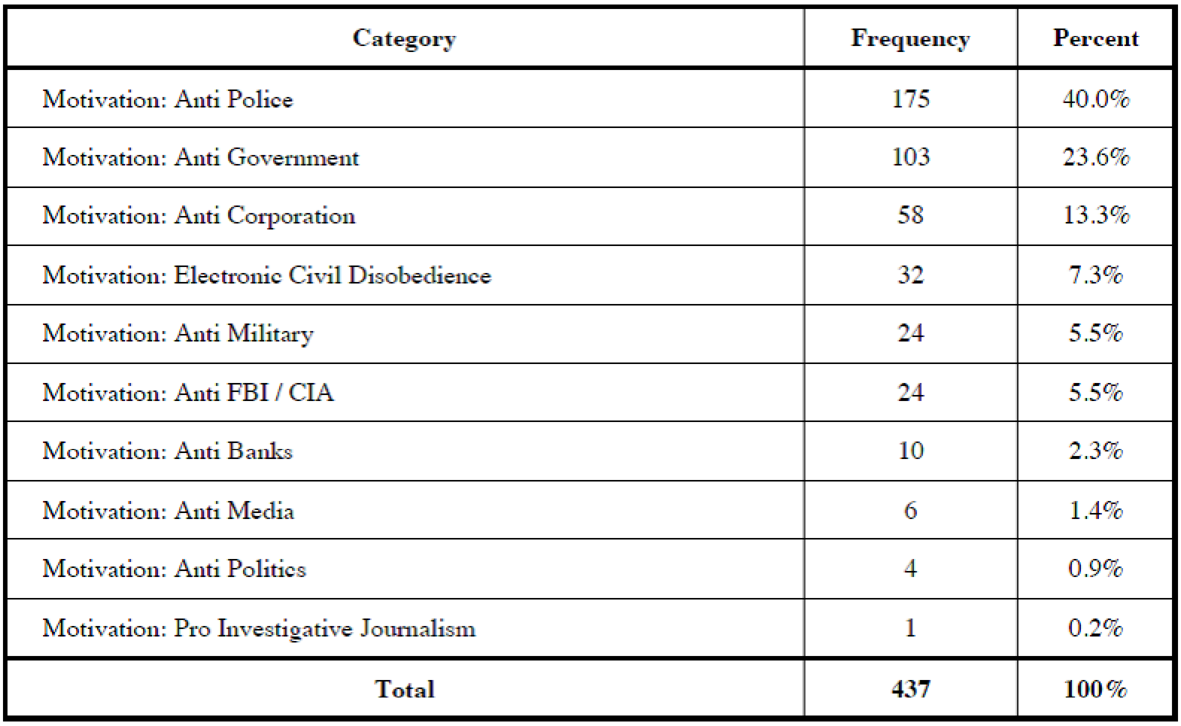


Figure 2: Gender distribution among 37 suspects (case analysis)

At present, we do not hold any reliable information about socio-economic characteristics. Case analysis indicates that most of the suspects are pupils, students and trainees, which would also correspond to the predominant age group of hacktivists. The preferred modi operandi employed by hacktivists are website defacement, DDoS attacks, data espionage and manipulation. Governments (and their members) and companies are most affected by hacktivism, although private individuals represent the majority of victims in case analysis, which can be put down to the companies' reporting behaviour.



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%**

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

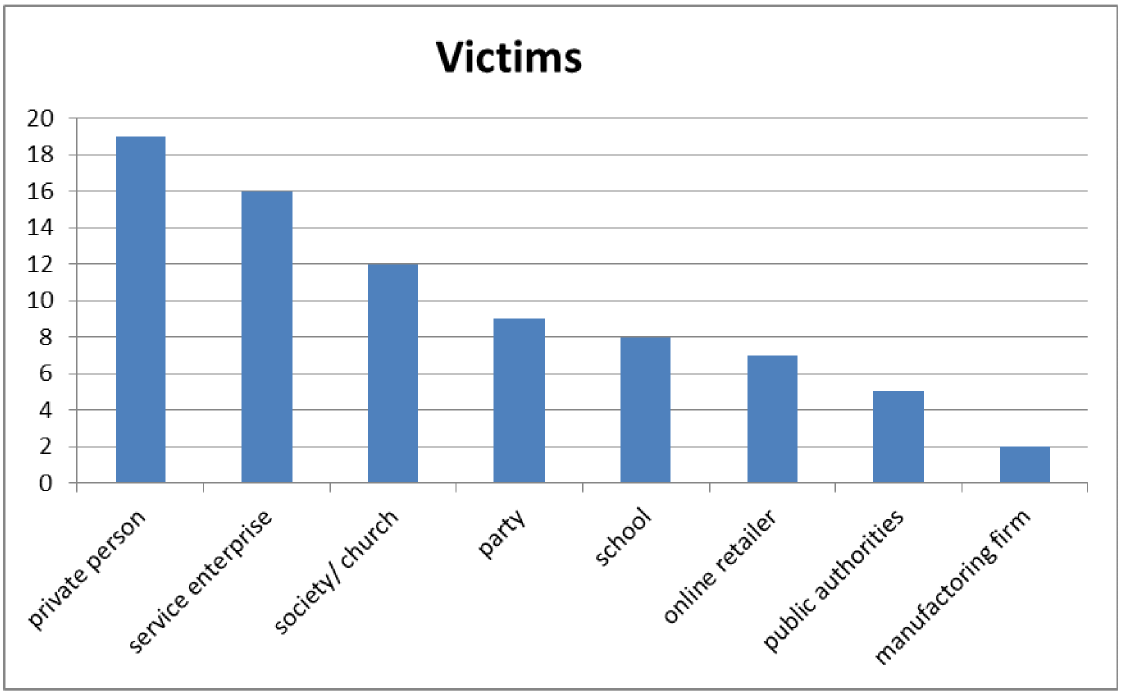


Figure 4: Victims in 78 cases (case analysis)

80 of the 971 companies taking part in the online survey stated that they had been affected by hacktivism on one or more occasions. This means that the frequency with which companies and public institutions in Germany are targeted by hacktivism is 8 %. It is particularly companies from the information and communications branch which are affected by hacktivist attacks more frequently than average.

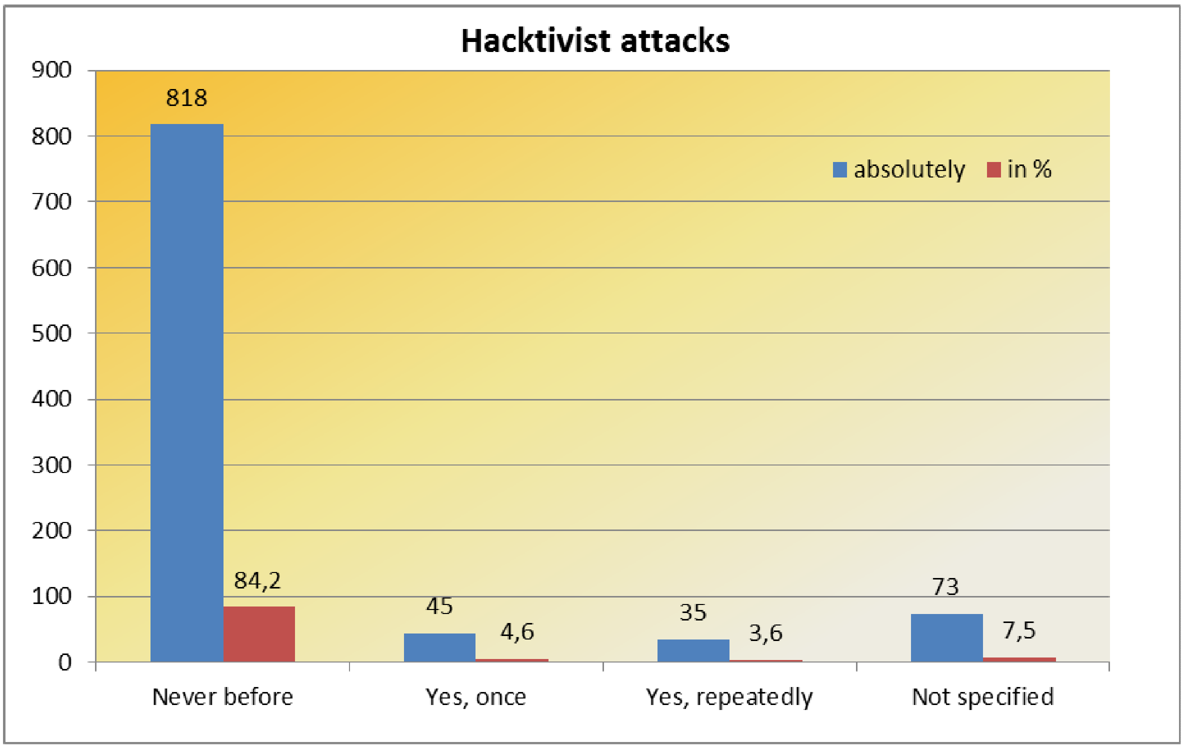


Figure 5: Hacktivist attacks on companies and public institutions (online survey)

The size of the company has an impact on the frequency of attacks: The bigger a company, the more likely it was affected by repeated hacktivist attacks. 60 % of the institutions affected fixed the damages internally; 15 % filed a complaint. When asked for the reasons for refraining from a complaint, 33 % of the companies stated that the attacks did not have any consequences, although an ineffective attack may also be punishable. 40 % did not expect a complaint to be successful. As regards unreported and unrecorded crime in the field of hacktivism, these results mean that the reporting rate for hacktivist attacks is 15 %, which implies that 85 % of detected activities go unreported and unrecorded (68 cases). Cases which are not detected by the victims must also be assigned to this dark field (absolute dark field).

All in all, media research has corroborated the fact that hacktivism also plays a role in the darknet: A discussion about the creation of a new hacktivist group was followed in the forum "Deutschland im Deep Web" ("Germany in the Deep Web"); the outcome of which, however, remained open. The sites "Hack the Planet" and "CODE GREEN" also deal with the subject of hacktivism. But only the "Deutschland im Deep Web" forum showed a clear link to Germany.

The assessment of the threat and damage potential of cybercrime phenomena is particularly dependent on the target and the modus operandi used by the offender. Although the threat and damage potential of hacktivism can currently be regarded as low, it becomes apparent that hacktivism is increasingly taking the form of "combined attacks", which means that experts with "hacking skills" are joining forces with social engineering experts and attack companies via social media to a larger extent.[2] Companies and institutions using social media should have the relevant competence for handling emerging conflicts to prevent such situations from culminating in hacktivist attacks.

There is no doubt that information and communications technology and the internet open up new effective spheres of activity and possibilities for activists. Not only can activities be planned and carried out faster, but the range of potential sympathisers targeted is also bigger due to the high acceptance and extensive use of the internet and social media; access to the users has become easier and more resource-efficient. Even persons who are politically interested but have not been very active so far now have the possibility to participate in the relevant activities in a quick and uncomplicated manner, since potential obstacles, which come along with analogue forms of protest, such as weather conditions, travel to an event, unwanted detection (if the participant is sufficiently anonymised) are virtually excluded when activities are carried out digitally. Only a mouse click is needed to participate in such a "demonstration". Most users, however, are not aware of the fact that the DDoS attack they may trigger in that moment constitutes a criminal offence. Citizens' and internet users' risk perception and

[2] This is even demonstrated in the case of massive internet outrage, which may result in conspiracies to commit attacks of a hacktivist nature.

media literacy must be developed in a way for them to know which offences committed on the internet are punishable.

Neither the results of secondary and case analysis nor of media research and the online survey indicate that hacktivist attacks have a significant threat potential. This applies to both recorded and unrecorded crime. The figures for losses do not suggest that hacktivism has a high damage potential, at least as far as attacks on victims in Germany are concerned. It must be assumed that, given the appropriate organisation and communication for the recruitment of sympathisers, hacktivist activities and attacks will rather increase than decrease in the future.

Table of Figures

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/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

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

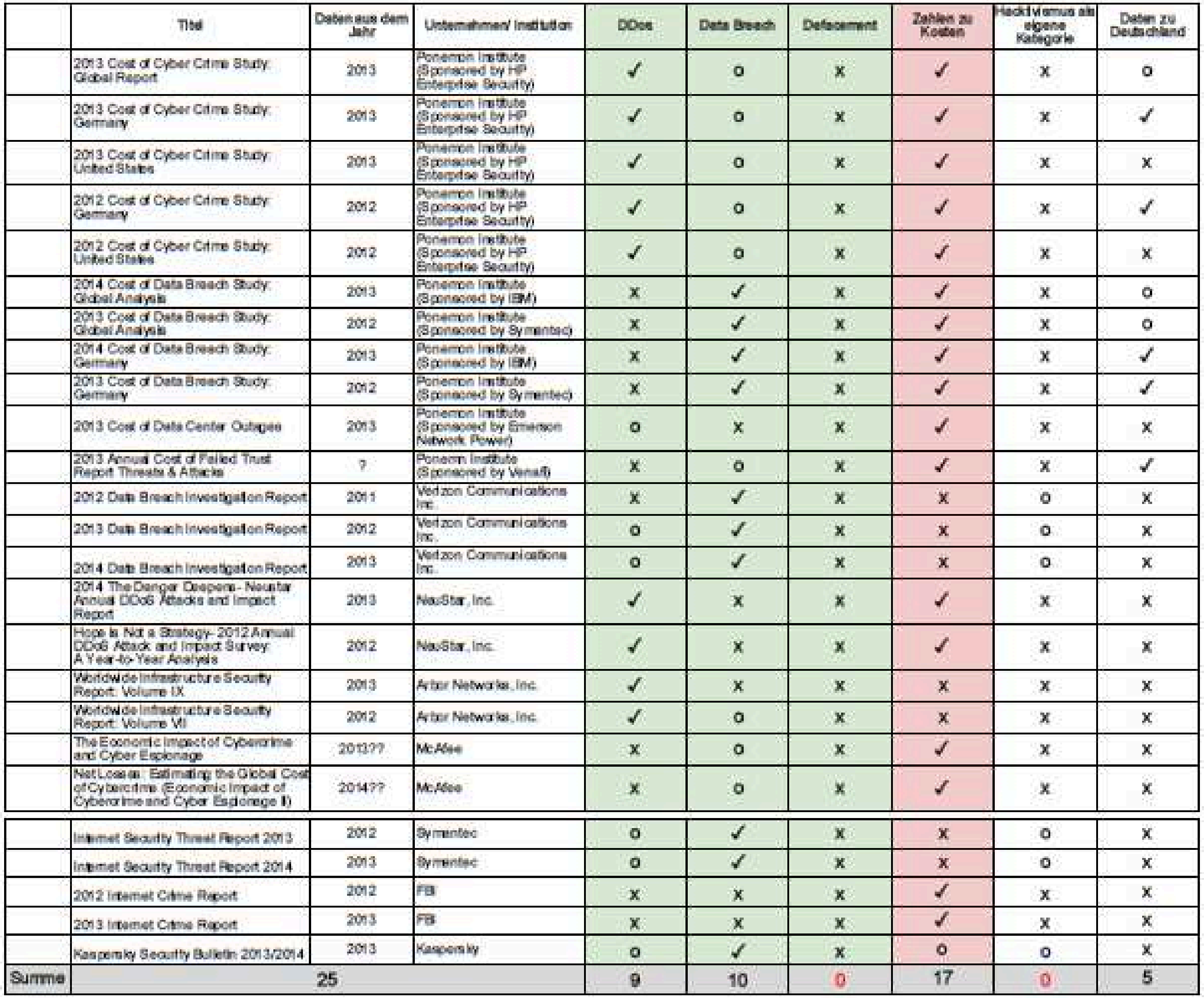
The Knightmare/Branwyn, G. (1994). *Secrets of a Super Hacker*. Loompanics Unlimited

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	?	Poneom 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.