26. Feb. 2015

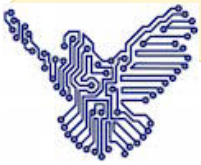
von gast

in Cyber Security

Kommentare (3)

Hacktivismus = Cybercrime? Eine Replik auf die Studie des BKA zu Hacktivisten

von Adrian Haase und Theresa Züger



Part VII of our series on cyberpeace

Vor wenigen Tagen veröffentlichte das Bundeskriminalamt eine Studie mit dem Titel „Hacktivisten„ die auf einem dreistufigen Forschungsdesign beruht: einer Literaturrecherche, einer quantitativen Fallauswertung von 78 polizeilich bekannten deutschen Fällen und einem Expertenarbeitstreffen, bei welchem Erfahrungswerte ausgetauscht wurden. Beginnen wir mit einer logischen Denksportaufgabe:

In der Einleitung wird folgende Prämissen aufgestellt:
1. „Hacktivismus (ist) (..) letztlich nichts anderes als die digitalisierte Form von Aktivismus." (BKA, 2015: 1)

Im Verlauf der Studie lässt sich wiederkehrend eine weitere Prämisse finden:
2. Hacktivismus ist eine Form von Cybercrime (vgl. BKA, 2015: z. B. 2).

Frage: Zu welcher Konklusion führen diese beiden Prämissen über Aktivismus?

Die zwei möglichen Antworten hier sind: Aktivismus ist ebenfalls eine Form der Kriminalität. Oder aber: Aktivismus wird zumindest dann kriminell wenn er digital ausgeübt wird. Beide Konklusionen verdeutlichen eine Problematik, die sich konsistent durch die Studie zieht: eine eingeschränkte Sichtweise auf Hacktivismus als kriminellen Akt. Dennoch ist dieser Fokus keine Überraschung, da er dem Erkenntnisinteresse des BKA entspricht. Aus Sicht des BKA könnte man argumentieren, dass man so versucht seinen Job zu machen, indem man sich auf strafrechtlich relevante Fälle konzentriert. Wir wiederum möchten unseren Job machen, die Studie wissenschaftlich hinterfragen und sie vor dem Hintergrund bestehender Forschung einordnen, um mögliche politische Implikationen aufzuzeigen.

Der paradoxe symbolische Kampf um den Hacktivismus

Auch wenn dies teilweise anders rezipiert wurde, scheint das BKA um eine Abgrenzung des Hacktivismus von den Begriffen Cyberwar und Cyberterrorismus bemüht. „Die wichtigste Abgrenzung zu Hacktivismus liegt im Ziel des Terrorismus begründet, nämlich Gewalt auszuüben, um einzuschüchtern und Schrecken und Leid zu verbreiten. So fällt eine Attacke, die Services unterbricht, aber nicht mehr als finanzielle Kosten verursacht, **nicht** darunter" und weiter:

> *„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" (BKA, 2015: 22,25 unsere Hervorhebung).*

Was für das BKA aber anscheinend nicht zur Debatte steht ist das Verständnis von Hacktivismus als kriminellem Akt. Besonders paradox fällt diese einseitige Sicht durch den Widerspruch mit einer Definition von Alexandra Samuels auf, die das BKA selbst anführt, in dem sie Hacktivismus beschreibt als „Hochzeit von politischem Aktivismus und Computerhacking [...] als den gewaltfreien Gebrauch von illegalen oder **legalen** digitalen Werkzeugen um politische Ziele zu verfolgen." (BKA, 2015: 21 unsere Hervorhebung)

CC BY-ND 2.0 by Dennis Skley

Dieser symbolische Konflikt um die Besetzung des Begriffs des Hacktivimus ist jedoch keine Neuheit und wird seit über 10 Jahren in der wissenschaftlichen Literatur thematisiert. Er vollzog sich als ähnliche semantische Entwicklung bereits mit dem „Hacking". Beide Begriffe erfahren von staatlicher Seite und teilweise auch in den Medien eine Neu-Besetzung als sicherheitspolitisch relevante Gefahren und kriminelle Tätigkeiten (ein Thema mit dem sich unser Fellow Leonie Tanczer auseinandersetzt). Ironischerweise weist das BKA selbst auf die ursprüngliche Neutralität des Begriffs des Hackens hin (BKA, 2015: 21) und schlägt dennoch in die selbe Kerbe der Kriminalisierung. Was kriminell ist und was nicht, verändert sich in einem politischen Anpassungsprozess, der im Moment in einer kritischen Phase zu sein scheint.

Mit dieser schleichenden begrifflichen Verschiebung hin zur kategorischen Kriminalisierung von Hacktivismus stehen zwei Probleme im Raum. Es ist zu befürchten, dass nach dem Hacking (§ 202c StGB wird in Wissenschaft und Praxis mittlerweile flächendeckend als sog. Hacking-Paragraph bezeichnet), auch der Begriff des Hacktivismus durch staatliche Institutionen als genuin strafrechtlicher Begriff besetzt wird. Damit wird ein Bild gezeichnet, das weder der Entstehung und der tatsächlichen Praxis von Hacktivismus noch dem Selbstverständnis von Hacktivsten gerecht wird. Einerseits besteht die Gefahr, dass völlig legale Formen, die in das Feld des Hacktivismus fallen, schneller unter Kriminalitätsverdacht stehen. Das betrifft etwa manche fiktive Netzkampagnen (wie jene der The Yes Men oder des Zentrums für politische Schönheit), Keyword Storms (wie das sogenannte Eschalon Bashing) oder das massenhafte Versenden persönlich verfasster Protestmails (wie in diesem Fall an den Axel Springer Verlag). Andererseits kann sich ein Abschreckungseffekt entwickeln: Wer glaubt, dass jede Art des Hacktivismus strafrechtlich verfolgt oder beobachtet wird, ist möglicherweise auch abgeschreckt an legalen Aktionen teilzunehmen. Dies könnte zu einem Klima der Angst für digitale Aktionen führen und letztlich die Meinungsfreiheit

und "Wir" – zu den Ambivalenzen im aktuellen Flüchtlingsdiskurs

Ich bin Paris! Ich bin Muslim! Ich bin Nato? Die offene Gesellschaft und ihre Feinde nach dem 13. November.

Hilfspaket für deutsche Medien – Annäherungen an unser Bild vom Pleite-Griechen

Der Dschihad der Auslandskämpfer: Ausdruck einer Subkultur

Terroristen oder Bürgerkriegsflüchtlinge? Was wir gegen diese Verwechslung tun müssen

KATEGORIEN

Außenpolitik (64)
Bürgerkriege (24)
Cyber Security (52)
Demokratisierung (14)
Drohnen (15)
Flüchtlinge (17)
Humanitäre Interventionen (15)
Innere Sicherheit (32)
Interviews (10)
Katastrophen (4)
Konferenz (29)
Militär (31)
Pandemien (2)
Podcast (7)
Popkultur (22)
Raketenabwehr (1)
Sanktionen (8)
Security Culture (27)
Sicherheits-Kommunikation (16)
Sicherheitskultur (237)
Sozialwissenschaft Online (71)
Stellenangebote (55)
Strategie (12)
Terrorismus (60)
Theorie (5)

massiv beeinträchtigen.

Immerhin auf der letzten Seite der Studie wird auch die Möglichkeit des zivilen Ungehorsams im Netz erwähnt. Für zivilen Ungehorsam – also einen absichtlichen, prinzipienbasierten, kollektiven – und nicht kriminell motivierten – Rechtsbruch, der das Ziel verfolgt, politische Maßnahmen zu beeinflussen (vgl. Celikates 2010: 280) – bleibt jedoch faktisch kein Platz, weil das Risiko für Aktivisten kaum abzusehen ist. Aus demokratischer Sicht macht es einen Unterschied, ob Hacktivismus politische Werte vertritt, die mit unseren Grundrechten und Freiheiten konform gehen – oder diese gerade durch den Protest einfordern – oder ob sie diesen widerstreben. Weder das BKA, noch die derzeitige Rechtsprechung, weisen jedoch auf eine solche Unterscheidung und ein politisches Feingefühl in der Praxis hin. Diese undifferenzierte Strafverfolgung, also die Tatsache, dass jede Form von Hacktivismus ohne Abstufung als Computerkriminalität bewertet wird, kann sich zusätzlich, durch manche Aspekte des Täterverständnisses des BKA und die formulierten Forderungen für ein zukünftiges Umgehen mit Hacktivisten verschärfen.

Hacktivisten als „die üblichen Verdächtigen“

Das BKA weist darauf hin, dass es sich zum jetzigen Zeitpunkt lediglich um eine sog. Hellfeldstudie handelt, die sich also mit den offiziellen Zahlen und Fakten beschäftigt, und daher ausschließlich entdeckte und in irgendeiner Art und Weise dem Strafverfolgungsprozess zugeführte hacktivistische Aktionen in die Untersuchung einbezogen worden sind. Vermutlich kommt deswegen der bereits erwähnten Expertengruppe eine prominente Rolle bei der Identifizierung und Einordnung von verdächtigen Hacktivisten zu. Über eine Analyse der untersuchten Fälle hinaus äußern die Mitglieder der Expertengruppe Vermutungen zum Wesen eines typischen Hacktivisten. Dieser sei nicht nur unbekannt, männlich und zwischen 18 und 30 Jahren alt (soweit decken sich Empirie und Erfahrungspraxis der Experten) sondern – laut Vermutung der Experten – zumeist Mitglied islamischer/islamistischer Gruppierungen, möglicherweise nachrichtendienstlich gelenkt und vor allem lediglich nebenberuflicher Hacktivist. Hauptberuflich seien diese (vermutlich) die „üblichen” Cyberkriminellen“ (BKA, 2015: 71).

Diese Vermutungen der Expertengruppe sind durchaus bemerkenswert. Aus wissenschaftlicher Sicht ist es problematisch solche Vermutungen unkritisch im Rahmen einer allgemeinen Studie zu veröffentlichen, ohne weitere Belege für diese Annahmen zu liefern und diese durch die empirischen Ergebnisse der Studie stützen zu können. Weiter zeigen sie einerseits den erstaunlich eindimensionalen Blickwinkel staatlicher Strafverfolgungsorgane auf eine Szene, die sich bislang einer pauschalen Einordnung erfolgreich entziehen konnte. Andererseits lassen sie Rückschlüsse auf zukünftig erwartbare Mittel und Maßnahmen zur präventiven und repressiven Bekämpfung von Hacktivismus zu. Vom Ausbau internationaler Kooperationen und Institutionen (Cybercrime-Abwehrzentrum bei Europol, Datenaustausch) über Strafrechtsharmonisierung, die Einführung der Vorratsdatenspeicherung bis hin zu Medienkampagnen zur Tätersensibilisierung hat das BKA den gesamten Strauß von *law and order* Maßnahmen im Programm. Eine Differenzierung zwischen strafrechtlich eindeutig relevantem Verhalten und erlaubten aktivistischen Online-Tätigkeiten findet nicht statt. Dies wäre aber nicht nur demokratietheoretisch geboten, da laut Richter und Verfassungsrechtler Ulf Buermeyer der Cyberangriff von heute morgen schon freie Meinungsäußerung sein könnte. Ein die Grundrechte schonendes Vorgehen des Staates und seiner Strafverfolgungsbehörden ist somit erforderlich. Darüber hinaus böte der differenzierte Blick auf hacktivistische Szenarien auch die Möglichkeit ressourcenschonender zu agieren und nicht jeden Akt

Umwelt (1)
Versicherheitlichung (23)
Visualisierung (6)
Whistleblowing (8)
WikiLeaks (17)
WMD (10)
Zivilgesellschaft (65)

BLOGROLL

Arbeitskreis soziale Bewegungen
Augen geradaus
Dan Drezner
Dart-Throwing Chimp
David Campbell
de.hypotheses.org
Demokratieforschung Göttingen
Duck Of Minerva
Future and Politics
Hylaean Flow
Internet und Politik
IR Blog
Just Security Blog
justsecurity.org
Killer Apps
Kings Of War
MPC Journal – Muslim Politics and Culture
netzpolitik.org
percepticon
shabka.org
Terrorismus in Deutschland
theorieblog.de
Verfassungsblog
Vom Bohren harter Bretter
whistleblower-net.de

ARCHIV

Wähle den Monat

des Hacktivismus wie einen Cyber-Großangriff zu behandeln.

Schadensberechnung leicht gemacht

Stutzig wird nicht nur der Jurist bei der Schadensberechnung. Das BKA beruft sich in seiner Studie hier auf Angaben des renommierten Kaspersky Lab und gibt die Schäden bei Großunternehmen mit 1.82 Millionen Euro und bei mittleren und kleinen Unternehmen mit 70.000 Euro pro Angriff an. Interessant sind weniger die Zahlen von Kaspersky Lab sondern vielmehr die Interpretation des BKA (BKA, 2015: 45f.). Es wird in der Studie zwar eingeräumt, dass die als Hacktivismus eingeordneten Fälle zumeist keine oder nur sehr geringe wirtschaftlich bezifferbare Schäden verursacht haben, dennoch wird auf die Zahlen von Kaspersky Lab Bezug genommen, obwohl diese in keinerlei Verbindung zum Hacktivismus stehen sondern ausdrücklich Cyber-Großangriffe betreffen und eine politische oder gesellschaftliche Dimension nicht erwähnen. Doch das BKA rückt Hacktivisten nicht nur abermals durch diesen Kunstgriff in die Richtung von Cyberkriminellen. Auch der auf den Angriff zurückgehende Schaden wird massiv erhöht, wenn „die Beseitigung von Schwachstellen“ als kausaler Schaden eingeordnet wird. Cyberkriminelle und/oder Hacktivisten werden auf diese Weise nicht nur für unmittelbare Schäden verantwortlich gemacht, die kausal auf ihre Angriffe zurückzuführen sind, sondern darüber hinaus auch für die Kosten, die durch eine Behebung von Schutzlücken in der IT-Sicherheit entstehen. Man darf also durchaus gespannt sein, wann der erste Einbrecher für eine defekte Alarmanlage, die seinen Einbruch ermöglicht hat, in Anspruch genommen wird...

Forschung zum Thema Hacktivsmus

Das BKA kommt zu der Einsicht, dass wissenschaftliche Untersuchungen zu Hacktivismus und Hacktivisten rar seien (findet aber selbst immerhin 184 Quellen). Zwar nicht zur bestehenden Forschung, jedoch zur Datengrundlage in Deutschland können wir bestätigen, dass die Erforschung von Hacktivismus mit Hürden verbunden ist.

Im Juli 2014 sendeten wir an sämtliche Oberstaatsanwaltschaften der Länder Anfragen bezüglich Ermittlungsverfahren, die möglicherweise im Kontext von Hacktivismus interessant sein könnten. Wir bekamen keinerlei dienliche Antwort, denn es bestehe „keine Möglichkeit die von (uns) gewünschten Daten hier abzufragen“, es sei aus „organisatorischen Gründen nicht möglich“, „Tathintergründe werden von staatsanwaltlicher Seite nicht erhoben“ oder es seien „keinerlei einschlägige Verfahren feststellbar“. Das BKA hatte im selben Zeitraum mit der Abfrage der Daten bei den Ermittlungsbehörden offensichtlich mehr Glück. Allerdings hinterlässt die Fallanalyse der ausgewählten 78 Fälle einige Fragen:

Weshalb macht das BKA in seiner Studie keine Angaben zu Verurteilungszahlen? Erst die gerichtliche Überprüfung und ein rechtsstaatlich festgestellter Verstoß gegen Strafnormen kann tatsächlich Aufschluss darüber geben, ob Hacktivisten sich durch ihre Aktionen strafbar gemacht haben, in welchem Ausmaß dies geschehen ist und welche Konsequenzen drohen. Die polizeiliche Einschätzung, dass ein Verhalten strafbar sei, sagt rein gar nichts über dessen wahren Charakter aus und sollte nicht zur Basis von zukünftigen Kriminalisierungs- und Strafverfolgungserfordernissen gemacht werden.

Die Sekundär- und die Fallanalyse divergieren erheblich bezüglich der Opfer von Hacktivismus, da sich die Prämissen der Literaturrecherche, dass Hauptgeschädigte Regierungen, Polizei und Unternehmen sind, mit den Erkenntnissen der Fallanalyse nicht vereinbaren lassen (BKA, 2015: 43). Wie

das BKA argumentiert, läge dies möglicherweise daran, dass viele Fälle nicht bekannt werden, da das Opfer einen Imageschaden befürchtet. Die fehlende Bereitschaft zur Anzeigeerstattung aus Imagegründen als einzige Erklärung ist hier mehr ein Feigenblatt, als eine Antwort und offenbart vielmehr, dass der in Deutschland bestehende Hacktivismus für das BKA mehr Fragen hinterlässt als Antworten sichert.

Was bleibt?

Die vorliegende Hellfeldstudie stellt lediglich den ersten Teil dar und soll zukünftig von einer Dunkelfeldstudie flankiert werden (BKA, 2015: 2, 81). Es bleibt also zu hoffen, dass sich das BKA von kritischen Anmerkungen inspirieren lässt, um dadurch dem vielschichtigen Phänomen des Hacktivismus besser gerecht zu werden. Unserer Ansicht nach ist dafür eine ergebnisoffenere Forschung hinsichtlich der Einordnung von Hacktivisten im Spannungsfeld zwischen politischer Meinungsäußerung, zivilem Ungehorsam und cyberkriminellen Aktivitäten geboten um dadurch eine demokratie- und ressourcenschonende Abstufung bei der ermittlungstaktischen Behandlung von Fällen zu erreichen.

Adrian Haase studierte Rechtswissenschaft an der Bucerius Law School in Hamburg und an der Stellenbosch University (Südafrika). Seit September 2013 ist er Doktorand im Doktorandenkolleg des Alexander von Humboldt Institut für Internet und Gesellschaft.

Theresa Züger studierte an der Universität zu Köln Theater-, Film- und Fernsehwissenschaft, Germanistik und Philosophie. Ihre Magisterarbeit befasste sich mit Internetethik und Internet Governance. Die Fragestellung ihrer Dissertation am HIIG behandelt digitalen zivilen Ungehorsam.

Tags: BKA, Cybercrime, Hacken, Hacktivismus, Hacktivisten, Kriminalisierung, ziviler Ungehorsam

« Der IS in den Medien und die Medien in der Strategie des IS
Das Dabiq-Magazin als Rekrutierungswerkzeug des IS »

Trackbacks/Pingbacks

1. **Hacktivismus = Cybercrime? Eine Replik auf die Studie des BKA zu Hacktivisten | netzpolitik.org** - 27. Feb. 2015

   [...] Artikel von Theresa Züger und Adrian Haase erschien gestern erstmals auf dem Sicherheitspolitik-Blog im Rahmen der Artikelreihe Cyberpeace: Dimensionen eines [...]

2. **Hacktivism = cybercrime? A reply to the Federal Criminal Office (BKA) study on hacktivists | Alexander von Humboldt Institut für Internet und Gesellschaft** - 2. Mrz. 2015

   [...] Previously published on sicherheitspolitik-blog.de and netzpolitik.org. [...]

3. **Hacktivismus = Cybercrime? Eine Replik auf die Studie des BKA zu Hacktivisten | Alexander von Humboldt Institut für Internet und Gesellschaft** - 2. Mrz. 2015

   [...] Artikel ist zuerst auf sicherheitspolitik-blog.de und netzpolitik.org [...]

Einen Kommentar hinterlassen

Name

Email

Webseite

Kommentar

Wählen Sie alle Bilder mit Straßennamen aus.

reCAPTCHA

Bestätigen

Soll die Herausforderung einfacher sein?

Kommentar senden

Benachrichtige mich über nachfolgende Kommentare per E-Mail.