Christina Gels

Anonymous und die Twitter-Konten des IS – Eine Diskussion über das Für und Wider der Deaktivierung IS-affiliierter Accounts

Kieler Analysen zur Sicherheitspolitik Nr. 46
September 2016

Inhalt:

Christina Gels, B.A.
Anonymous und die Twitter-Konten des IS –
Eine Diskussion über das Für und Wider der Deaktivierung IS-affiliierter Accounts
Kieler Analysen zur Sicherheitspolitik Nr. 46
Kiel, September 2016

Impressum:
Hrsg. von Prof. Dr. Joachim Krause und Stefan Hansen, M.A.
Institut für Sicherheitspolitik an der Universität Kiel gGmbH
Düsternbrooker Weg 77a
24106 Kiel

ISPK.org

1. Einleitung

Die Vorstellung, dass Terroristen in sozialen Netzwerken wie Twitter, YouTube und Facebook ungehindert ihre menschenverachtenden Botschaften verbreiten können, scheint für viele Menschen nicht hinnehmbar. Der ehemalige US-Senator Joseph Lieberman brachte diese Einstellung mit dem griffigen Appell zum Ausdruck, dass wir „den Cyberspace nicht den Terroristen überlassen dürfen."[1] Als praktische Konsequenz fordern etliche Akteure, terroristische Inhalte und ihre Verbreiter aus den sozialen Netzwerken zu entfernen – z.B. indem entsprechende Accounts auf dem Kurznachrichtendienst Twitter deaktiviert werden, welcher in den letzten Jahren zur bevorzugten Plattform von Dschihadisten wie dem IS geworden ist.[2]

Trotz entsprechender Forderungen ist es bisher noch nicht zu einer wirklich systematischen, großangelegten Deaktivierung von IS-affiliierten Twitter-Accounts gekommen – weder von der Seite des Betreibers noch von Regierungsseite. Eine Diskussion über das Für und Wider droht daher übermäßig spekulativ im „luftleeren Raum" stattzufinden. Um dies zu vermeiden nutzt der vorliegende Beitrag die Hackattacken des Netzwerks Anonymous als Fallstudie, ausgehend von der Annahme, dass jede systematische Kampagne zur Löschung von IS-Accounts vor ähnlichen Problemen und Abwägungen stehen würde. Ziel dieses Beitrages ist es, solche Attacken im Rahmen eines sicherheitspolitischen Diskurses einzuordnen und zu bewerten. Dies soll anhand der konkreten Fragegestellung erfolgen, ob die Hackattacken, die zumeist auf eine Deaktivierung IS-affilierter Social Media-Accounts abzielen, aus einer sicherheitspolitischen Überlegung heraus wünschenswert und im Kampf gegen den Terrorismus des IS dienlich sind.

Hierbei wird der Themenbereich folgendermaßen eingegrenzt: Es handelt es sich bei der vorliegenden Analyse um eine Fallstudie, die sich auf eine Untersuchung der Arbeit des Hackernetzwerkes Anonymous beschränkt und einen Fokus auf dessen zwei großangelegte Hackattacken im Jahr 2015 legt. Die Tätigkeiten von Geheimdiensten, die – wie man annehmen darf – ebenfalls die sozialen Medien beobachten und über die technischen Möglichkeiten verfügen, sie ggf. zu hacken, werden in diesem Beitrag mangels gesicherter Erkenntnisse nicht behandelt. Die Fragestellung klammert auch die – nichtsdestoweniger hochwichtige – Diskussion über das Thema der freien Meinungsäußerung in den sozialen Medien aus, die durch die Hackattacken beschnitten wird.

1 Broache, Anne: „Senators voice alarm over terrorist net presence", CNet News online, 04.05.2007, http://www.cnet.com/news/senators-voice-alarm-over-terrorist-net-presence/, (22.07.2016).

2 MEMRI: Jihadis' Responses To Widespread Decline In Participation On Jihadi Forums: Increased Use Of Twitter. MEMRI Inquiry & Analysis Series No. 955, März 2013.

2. Ereignis, Akteure und Problemstellung

Nach der Anschlagsserie vom Januar 2015, die unter anderem das Satiremagazin Charlie Hebdo traf, und nach den Attentaten von Paris am 13. November 2015 verkündete das Hackernetzwerk Anonymous, dass es einen groß angelegten Angriff auf die Social Media-Accounts von Terrororganisationen wie dem IS durchführen wolle.[3] Als Motivation für diese Attacken gab das Netzwerk an, den Tod der Journalisten und Zeichner von Charlie Hebdo rächen zu wollen, da sie den Anschlag auf das Satiremagazin als Angriff auf die Meinungsfreiheit verstanden.[4] Nach den Anschlägen von Paris im November starteten sie eine zweite Attacke mit dem Ziel, die Drahtzieher zu identifizieren sowie Rekrutierungs- und Finanzierungsströme des Netzwerkes offen zu legen.[5]

Im Rahmen der Kampagnen #OpCharlieHebdo und #OpParis (der zugehörige Twitter-Account zur ersten Aktion hatte mehr als 50.000 Follower, wurde aber bereits am 21. Januar 2015 von Twitter suspendiert) führte das Netzwerk unter anderem Attacken gegen IS-affiliierte Twitter- und Facebook-Accounts sowie Websites durch, um diese zu übernehmen oder zu deaktivieren, und teilte Listen mit den Namen verdächtiger Accounts und Websites über ihre eigenen Twitter-Konten.[6] Zudem meldete das Netzwerk Propagandavideos, die im Internet kursierten.[7]

Eine quantitative Erfolgsbemessung dieser Operationen scheint beispielsweise anhand von suspendierten Accounts möglich. So verkündete Anonymous am 19. Januar 2015 in seinem Account @AnonyOpNews, dass bereits 1.200 verdächtige Twitter-Konten sus-

3 Diverse Videos mit den Ankündigungen der Gruppe nach den Charlie Hebdo Anschlägen und den Attentaten von Paris finden sich auf YouTube, beispielsweise: „#OpCharlieHebdo, https://www.youtube.com/watch?v=eRsaMI8w8Ew, (19.07.2016); „#OpParis", https://www.youtube.com/watch?v=IThIa-nVGSI, (19.07.2016).

4 Auf Pastebin ist eine Abschrift der Ankündigung nach den Charlie Hebdo Anschlägen zu finden, die diese Informationen beinhaltet: „#OpCharlieHebdo", Pastebin, 07.01.2015, http://pastebin.com/Pdj2ZowC, (06.07.2016).

5 Vgl. o.V.: „'From Paris ... With Love' #IntelGroup Interviews @OpParisOffical #OpParis", Anonymous Intelligence Group online, o.D., http://www.anonintelgroup.com/2015/11/20/from-pariswith-love-intelgroup-interviews-opparisofficial-opparis/, (13.07.2016).

6 Vgl. Cuthbertson, Anthony: „Anonymous @OpCharlieHebdo account suspended by Twitter", International Business Times online, 22.01.2015, http://www.ibtimes.co.uk/anonymous-opcharliehebdo-account-suspended-by-twitter-1484597, (19.07.2016); vgl. Cuthbertson, Anthony: „Anonymous #OpCharlieHebdo campaign takes down 200 suspected jihadist Twitter accounts", International Business Times online, 14.01.2015, http://www.ibtimes.co.uk/anonymous-opcharliehebdo-campaign-takes-down-200-suspected-jihadist-twitter-accounts-1483372, (19.07.2016). Eine Liste verdächtiger Accounts findet sich auf Pastebin, 09.01.2015, http://pastebin.com/pfffWm3u, (19.07.2016).

7 Vgl. Kirst, Virginia: „Das könnte Anonymous gegen den IS ausrichten", Die Welt online, 16.11.2015, http://www.welt.de/wirtschaft/webwelt/article148922749/Das-koennte-Anonymous-gegen-den-IS-ausrichten.html, (07.07.2016).

pendiert worden seien.[8] Diese Angaben zu verifizieren gestaltet sich jedoch schwierig – auch für Anonymous selbst –, da die Zahlen aufgrund der losen Organisationsstruktur des Netzwerkes nicht eindeutig sind. Die Hackergruppe berichtete beispielsweise anhand des Accounts @OpParisOfficial am 17. November 2015, dass bereits 5.500 Twitter-Konten suspendiert worden seien,[9] während der Account @TheAnonMovement am gleichen Tag die Anzahl von suspendierten Accounts auf 6.000 bezifferte.[10] Zudem hält die #OpParis bis heute an, weshalb eine abschließende Bewertung noch aussteht. Laut eines Berichtes der Zeitung „Die Welt" vom 16. November 2015 gab Anonymous selbst an, seit der Einleitung der #OpCharlieHebdo 101.000 Twitter Accounts suspendiert, 149 Internetseiten deaktiviert und 5900 Propagandavideos gemeldet zu haben.[11] Weiterhin veröffentlicht das Netzwerk immer wieder Listen mit hunderten verdächtigen Twitter- und Facebook-Accounts, Email-Adressen und Internetseiten.[12]

An dieser Stelle scheint ein kurzer Blick auf die Rechtslage betroffener Social Media-Unternehmen nötig, um Angriffe auf Accounts generell juristisch einordnen zu können. Die Datenschutzrichtlinie Twitters[13] schreibt vor, dass das Unternehmen unter bestimmten Bedingungen Informationen über Nutzer offenlegen darf, etwa um geltende Gesetze zu erfüllen oder um gerichtlichen oder behördlichen Aufforderungen nachzukommen.[14] Weiterhin behält es sich das Recht vor – ist aber nicht verpflichtet! – innerhalb von Accounts Inhalte zu löschen sowie Nutzer zu sperren, Nutzernamen zu entziehen oder deren Accounts lahmzulegen. Dieses Recht kommt aber nur zur Anwendung, wenn Nutzer beispielsweise gegen die Twitter-Regeln verstoßen oder eine Gefahr oder ein mögliches rechtliches Risiko für das Unternehmen darstellen. Hacken, wie es beispielsweise Anonymous betreibt, ist in den Allgemeinen

8 Vgl. Tweet von @AnonyOpNews, 19.01.2015, https://twitter.com/anonyopnews/status/557095732218302464, (08.07.2016).

9 Die Twitter-Seite mit der offiziellen Meldung (https://twitter.com/opparisofficial/status/666553008541552640, 07.07.2016) ist nicht mehr zugänglich, diverse Zeitungen veröffentlichten aber Screenshots oder Abschriften, so beispielsweise: Crilly, Rob: „Anonymous ‚takes down thousands of Islamic State Twitter accounts'",The Telegraph online, 17.11.2015, http://www.telegraph.co.uk/news/worldnews/islamic-state/12002179/Anonymous-takes-down-thousands-of-Islamic-State-Twitter-accounts.html, (07.07.2016).

10 Vgl. Tweet von @TheAnonMovement, 17.11.2015, https://twitter.com/TheAnonMovement?ref_src= twsrc%5Etfw, (07.07. 2016).

11 Vgl. Kirst, „Das könnte Anonymous gegen den IS ausrichten".

12 Verdächtige Twitter- und Facebook-Accounts sowie Mailadressen und Websites wurden am 08.02. veröffentlicht: „#OpISIS. Exposed & Destroyed By Anonymous", Pastebin, 08.02.2015, http://pastebin.com/jdm2JK5s, (08.07.2016). Am 15.11. folgte eine Liste mit 911 verdächtigen Twitter-Accounts: „Hundreds of ISIS Accounts", Pastebin, 15.11.2015, http://pastebin.com/N9rPZ3Ar, (08.07.2016).

13 Da sich Anonymous mit seinen Hackattacken hauptsächlich auf Twitter-Accounts fokussiert, soll dieses soziale Medium und damit das Unternehmen Twitter im Mittelpunkt der Analyse stehen.

14 Vgl. Twitter: Datenschutzrichtlinie. Austausch und Offenlegung von Informationen. Recht und Rechtsverletzungen, Twitter, 27.01.2016, https://twitter.com/privacy?lang=de, (07.07.2016).

Geschäftsbedingungen als deutlich rechtswidriger Akt ausgewiesen.[15]

Durch die eher lockere Umsetzung dieser Geschäftsordnung geriet Twitter 2015 heftig in Kritik. Dem Unternehmen wurde vorgeworfen, dass es ein Laissez-faire Prinzip verfolge, was die unangemessene Nutzung der Plattform durch den IS und Sympathisanten betraf.[16] Vor diesem Hintergrund sind auch staatlichen Behörden die Hände gebunden: Diesen ist es offiziell nur möglich, rechtliche Anfragen zu stellen, wie etwa Aufforderungen zur Aufbewahrung von Daten[17], Auskunftsanträge[18] und Entfernungsanträge[19]. Solchen Anträgen ist Twitter aber beispielsweise nach eigenen Angaben in der ersten Hälfte 2015 weder in den USA noch in Großbritannien nachgekommen.[20]

Vor dem Hintergrund dieses Laissez-faire Prinzips, das Twitter noch 2015 verfolgte, und der begrenzten staatlichen Möglichkeiten für einen Eingriff, leitete das Netzwerk Anonymous die beiden großangelegten Hackattacken ein. Dies wirft folgende Frage auf: Ist das Deaktivieren von Twitter-Accounts, wie es durch Angriffe von Hackernetzwerken wie Anonymous erfolgt, eine erfolgversprechende Maßnahme?

3. Diskussion

In der folgenden Diskussion sollen zuerst Argumente, die für eine Deaktivierung von Accounts sprechen, analysiert werden. So wird beispielsweise argumentiert, dass durch Suspendierungen von Twitter-Konten der Kontakt zwischen Rekrutierern und Rekruten unterbrochen wird. Dies erhöht die Anstrengung, die nötig ist, um IS-Propaganda zu konsumieren – und reduziert dementsprechend die Zahl derer, die dazu bereit und in der Lage sind.[21] Allerdings werden Propaganda- und Rekrutierungsströme auf diese Weise immer nur kurzfristig unterbrochen, da die meisten Nutzer nach einer Deaktivierung mit neu ge-

15 Vgl. Twitter: Allgemeine Geschäftsbedingungen. Einschränkungen in Bezug auf Inhalte und die Nutzung der Dienste. Punkt 8. Twitter online, 27.01.2016, https://twitter.com/tos?lang=de#restrictions, (07.07.2016).

16 Vgl. Broomfield, Matt: „Twitter shuts down 125,000 Isis-linked accounts", Independent online, 06.02.2016, http://www.independent.co.uk/life-style/gadgets-and-tech/news/125000-isis-linked-accounts-suspended-by-twitter-a6857371.html, (08.07.2016); vgl. Waddell, Kaveh: „Twitter's Account Suspensions Are Surprisingly Effective Against ISIS", The Atlantic online, 19.02.2016, http://www.theatlantic.com/technology/archive/2016/02/twitters-account-suspensions-are-surprisingly-effective-against -the-islamic-state/463440/, (08.07.2016).

17 Vgl. Twitter: Guidelines for law enforcement. Twitter, ohne Datum, https://support.twitter.com/articles/20170305, (08.07.2016).

18 Vgl. Twitter, Guidelines for law enforcement.

19 Vgl. Twitter: Country withheld content. How Can I Request to Have Content Withheld? Twitter, ohne Datum, https://support.twitter.com/articles/20170926, (08.07.2016).

20 Vgl. Twitter: Transparency Report. Removal requests. Twitter, ohne Datum, https://transparency.twitter.com/removal-requests/2015/jan-jun (08.07.2016).

21 Vgl. Berger, J.M.: „The Evolution of Terrorist Propaganda. The Paris Attack and Social Media." Beitrag der Brookings Foundation, 27.01.2015, http://www.brookings.edu/research/testimony/2015/01/27-terrorist-propaganda-social-media-berger, (11.07.2016).

gründeten Accounts zurückkehren.[22] Zudem treffen solche Suspendierungen dauerhaft auch nur die am wenigsten involvierten Individuen, die dann aus dem jeweiligen sozialen Medium verbannt werden, während stärker radikalisierte Follower mit einem neuen Account zurückkehren.[23]

Vor dem Hintergrund, dass der IS Twitter-Accounts nutzt, um Follower und andere Accounts auszuspionieren, erscheinen Deaktivierungen als geeignete Maßnahme, um diesen Strom der Informationsbeschaffung zu unterbrechen.[24] Außerdem gab ein Anonymous-Hacker, der hinter der #OpParis steht, in einem BBC-Interview an, dass Deaktivierungen auch die Planung von terroristischen Anschlägen erschwerten.[25] Einige Wissenschaftler sind zudem der Meinung, dass das Deaktivieren Finanzströme unterbreche, da der IS soziale Netzwerke auch für Fundraisung nutze.[26] Diese Argumente können allerdings als fraglich gelten, da ein soziales Medium wie beispielsweise Twitter, das von öffentlichen Posts lebt und wenig Raum für private Konversationen bietet, sich nur sehr bedingt zur Planung von Anschlägen oder zur Finanzierung eignet. Primär werden Leute dazu motiviert, zu spenden oder selbst terroristisch zu agieren – es handelt sich also im weitesten Sinne immer noch um Propaganda.

Allerdings kam eine Brookings Studie zu dem Ergebnis, dass mittlerweile acht Prozent der jetzigen Online-Aktivitäten von IS-Mitgliedern darauf verwendet wird, ihr Netzwerk an Twitter-Konten nach einer Suspendierung wieder herzustellen. Dies nimmt viel Zeit in Anspruch, da beispielsweise ehemalige Follower wieder „gewonnen" werden müssen und spricht – allein aufgrund der gebundenen Ressourcen – für einen positiven Effekt von Account-Deaktivierungen. Ebenso ist festzustellen, dass die Geschwindigkeit, mit der Twitter-Konten wiederhergestellt werden, hinter der Geschwindigkeit, mit der sie deaktiviert werden, zurückbleibt.[27]

Scott J. White, außerordentlicher Professor für nationale Sicherheit an der Drexel Universität, betont zudem einen psychologischen Aspekt dieser Maßnahme: Durch das Deakti-

22 Vgl. Berger, J.M./Morgan, Jonathan: The ISIS Twitter Census – Defining and describing the population of ISIS supporters on Twitter. The Brookings Project on U.S. Relations with the Islamic World Analysis Paper, 20.03.2015, S. 56.
23 Vgl. Fisher, Ali/Prucha, Nico: „ISIS Is Winning the Online Jihad Against the West", The Daily Beast online, 10.01.2014, http://www.thedailybeast.com/articles/2014/10/01/isis-is-winning-the-online-jihad-against-the-west.html, (11.07.2016).
24 Vgl. Interview mit Gabriel Weimann: „Terrorist groups recruiting through social media", CBC News online, 10.01.2012, http://www.cbc.ca/news/technology/terrorist-groups-recruiting-through-social-media-1.1131053, (19. 07.2016).
25 Vgl. Cellan-Jones, Rory: „Anonymous takes on IS", BBC online, 17.11.2015, http://www.bbc.com/news/technology-34850573, (13.07.2016).
26 Vgl. o.V.: ISIS. Portrait of a Jihadi Terrorist Organization. Beitrag des Meir Amit Intelligence and Terrorism Information Center, November 2014, S. 202; vgl. Jacobsen, Michael: Terrorist Financing and the Internet. Beitrag des Stein Program on Counterterrorism and Intelligence, The Washington Institute for Near East Policy, März 2010.
27 Vgl. Berger/Morgan, The ISIS Twitter Census. S. 55.

vieren von Accounts zeige Anonymous, dass der IS nicht so unverletzlich sei, wie die Organisation es selbst gerne darstelle. Diese Offenlegung von Schwäche habe teils einen abschreckenden Effekt auf potenzielle Rekruten.[28]

Nach dieser Übersicht von Argumenten, die ein Deaktivieren von Twitter-Accounts befürworten, folgt nun eine Analyse der Gegenargumente. So muss beispielsweise darauf hingewiesen werden, dass IS-Mitglieder immer einem Kreislauf folgen: Wird einer ihrer Accounts deaktiviert, werden schlicht neue Konten eröffnet.[29] Dabei kann auch nicht davon ausgegangen werden, dass wertvolle Daten abhandenkommen, da sich der IS online in Form eines „Swarmcast" organisiert. Wie in Schwärmen ausfliegend verbreitet sich beispielsweise ein Video anhand diverser IS-Twitter-Accounts. Eine Deaktivierung des Urheber-Accounts erscheint bei dieser Organisationsstruktur nutzlos, da der Video-Link in dem Moment der Suspendierung schon weit gestreut ist. Nicht nur die Geschwindigkeitskomponente gereicht dem IS im Swarmcast-Modell zum Vorteil. Durch Querverbindungen zwischen IS-Accounts wird auch eine Widerstandsfähigkeit gegen Datenverlust durch Deaktivierungen erreicht.[30] Diese Widerstandsfähigkeit wird noch vergrößert, da IS-Unterstützer in ihren Tweets zumeist populäre und aktuelle Hashtags, wie beispielsweise #FIFAWorldCup, verlinken. Eine Verbindung mit diesen Tweets ermöglicht zudem Zugang zu einem noch größeren Publikum.[31]

Beide Komponenten verhelfen dem IS, eine persistente Online-Präsenz zu erhalten. Ein Beispiel verdeutlicht diesen Sachverhalt: Prucha hat anhand des 2014 veröffentlichten IS-Videos, das die Verbrennung des jordanischen Piloten Mu'adh al-Kasasiba zeigt, errechnet, dass 6.826 Accounts, die miteinander durch 17.713 Retweet-Verbindungen verknüpft sind, zeitgleich gelöscht werden müssten, um eine Ausbreitung des Videos zu verhindern. Aufgrund dieses Beispiels wird deutlich, dass es strategisch wichtig ist, nicht die aktivsten Accounts – also die mit den meisten Tweets – zu löschen, sondern jene zu überwachen, die häufig retweeted werden.[32] Dies erklärt sich aufgrund der Tatsache, dass Tweets eines Autors lediglich isoliert im Netz stehen, wenn sie nicht retweeted, also von

28 Vgl. Mastroianni, Brian: „Anonymous vs. ISIS. Who has the upper hand in social media war?" CBS News online, 24.11.2015, http://www.cbsnews.com/news/anonymous-vs-isis-social-media-war/, (13.07.2016).
29 Vgl. Berger/Morgan, The ISIS Twitter Census. S. 56.
30 Vgl. Prucha, Nico: „Turning the Volume Up to 11 is not Enough (part 2). Networks of Influence and Ideological Coherence." Beitrag auf Jihadica.com, 23.03.2015, http://www.jihadica.com/turning-the-volume-up-to-11-is-not-enough-part-2-networks-of-influence-and-ideological-coherence/, (11.07.2016).
31 Vgl. Fisher, Ali: „Eye of the Swarm. The Rise of ISIS and the Media Mujahedeen", Beitrag des USC Center on Public Diplomacy online, 08.07.2014, http://uscpublicdiplomacy.org/blog/eye-swarm-rise-isis-and-media-mujahedeen (11.07.2016).
32 Vgl. Prucha, „Turning the Volume Up to 11 is not Enough (part 2)".

anderen Nutzen geteilt und somit weiter verbreitet werden.

Der IS profitiert aber nicht nur von der Swarmcast-Organisationsstruktur, er nutzt auch eine Multiplattform-Strategie. So sind Unterstützer der Terrororganisation nicht nur in vielen unterschiedlichen sozialen Medien aktiv (Facebook, Twitter, YouTube etc.), wo sie über eigene Veröffentlichungen in den jeweils anderen sozialen Medien berichten und so diverse Accounts in unterschiedlichen sozialen Netzwerken miteinander verknüpfen; auch berichten andere Medien regelmäßig über Neuerscheinungen von IS-Propagandamaterial.[33]

Auch die Anpassungsfähigkeit, die IS-Unterstützer an den Tag legen, führt dazu, dass Deaktivierungen von Twitter-Accounts nicht immer den gewünschten Effekt erzielen. So verlegen Anhänger der Terrororganisation ihre Accounts zunehmend in solche sozialen Medien, die eventuell nicht so populär sind, dafür aber weniger strikte Nutzungsregeln vorgeben.[34] Das russische Netzwerk VK.com wird mittlerweile vom IS so effizient genutzt, dass sich die Organisation dort eine Art Bibliothek aufbauen konnte, die das dauerhafte Speichern von Inhalten ermöglicht. Dieses Netzwerk ist wiederum mit Google+ und Twitter-Accounts verknüpft, womit die Multiplattform-Strategie weiter fortgesetzt wird. Wird also beispielsweise ein Twitter-Account gelöscht, kann er sich durch die Unterstützung anderer Twitter-Accounts, die z.B. den neuen Account-Namen retweeten, und sogar durch die Unterstützung von Accounts in anderen sozialen Medien neu konfigurieren.[35]

Anpassungsfähigkeit beweist der IS nicht nur durch das Ausweichen auf andere soziale Medien – die Organisation verschickte per Twitter und JustPaste.it Regeln, an die sich IS-Anhänger halten sollen, damit ihre Accounts nicht suspendiert werden. Diese Regeln gaben zum Beispiel vor, Benutzernamen im Zehnminutentakt zu ändern.[36] Dieses Argument kann allerdings auch für eine Deaktivierung sprechen. Suspendiert man entsprechende Twitter-Accounts, ist es auch nicht mehr möglich, Regeln zum Schutz dieser Konten zu verschicken.

Um Netzwerke wie den IS, die sich in dieser Art formieren, online bekämpfen zu können, benötigen Gruppen wie Anonymous exakte Kenntnisse darüber, wie Informationen und Propaganda des IS ausschwärmen, das Internet durchdringen und ihren Bekämpfungsmaßnahmen entkommen. Nur wenn sie über

33 Vgl. Fisher /Prucha: „ISIS Is Winning the Online Jihad Against the West".
34 Vgl. o.V., ISIS. Portrait of a Jihadi Terrorist Organization, S. 209.
35 Vgl. Fisher /Prucha: „ISIS Is Winning the Online Jihad Against the West".
36 Das JustPaste.it-Dokument scheint bereits gelöscht worden zu sein, die Abschrift einiger Passagen findet sich aber hier: Intelligence Group Jihadist Threat: „IS Supporter Suggests Method to Avoid Twitter Suspension", Intelligence Group, 14.11.2015, https://news.siteintelgroup.com/Jihadist-News/is-supporter-suggests-method-to-avoid-twitter-suspension.html, (13.07.2016).

diese Kenntnisse verfügen, können systematische Deaktivierungen dem IS wirklich Schaden zufügen. Dass sich Anonymous aber der Feinheiten dieser Organisationsstruktur bewusst ist, darf bezweifelt werden.

Weiterhin wird die Effizienz von Deaktivierungen von Twitter-Accounts infrage gestellt, weil der IS noch andere Wege nutzt, um seine Propaganda zu verbreiten. Das IS-Online-Magazin Dabiq ist beispielsweise frei im Internet zugänglich.[37]

Auch das U.S. Department of Homeland Security (DHS) steht Deaktivierungen von Twitter Accounts kritisch gegenüber. In einem von der Behörde veröffentlichten Bericht wird auf den Zusammenhang hingewiesen, dass das Blockieren von Accounts und der daraus resultierende Strafverfolgungsdruck, den Inhaber suspendierter Twitter-Konten verspüren, dazu führe, dass sich diese entschließen, Anschläge im Inland zu verüben.[38] Da zum einen keine weiteren Quellen auf diesen Zusammenhang hinweisen und da zum anderen das DHS selbst keine Statistiken zu Attentaten, die als Reaktion auf eine Account-Deaktivierung verübt wurden, veröffentlicht hat, bleibt diese Auswirkung einer Twitter Suspendierung jedoch fragwürdig.

In einer Diskussion, die Argumente für und wider der Deaktivierung von IS-affilierten Twitter-Accounts abwiegt, darf auch der wichtige Faktor der Informationsbeschaffung nicht ausgelassen werden. Behörden finden in Twitter-Konten, die mit dem IS in Verbindung stehen, Informationen, zu denen sonst kein Zugang bestünde.[39] So können beispielsweise Informationen abgegriffen werden, die zu einer Identifikation von IS-Mitgliedern führen kann. Dies erfolgt anhand von Informationen, die ein Nutzer in seinem Profil angegeben hat, etwa der Muttersprache oder des Herkunftslandes.[40] Anhand verwendeter Worte, eventueller spezifischer Rechtschreibfehler und immer wiederkehrender Phrasen in Tweets ist relativ einfach herauszufinden, wie viele Accounts von einer einzigen Person betrieben werden; zudem kann man dieser Person eventuell einen Namen zuordnen, was eine Strafverfolgung ermöglicht.[41] Auch durch Filme und anderes Propagandamaterial, das vom IS in sozialen Netzwerken veröffentlicht wird, kann eine Identifikation von IS-Unterstützern

37 Hier findet sich z.B. eine Ausgabe des Magazins: Clarion Project, ohne Datum, http://media.clarionproject.org/files/islamic-state/islamic-state-dabiq-magazine-issue-7-from-hypocrisy-to-apostasy.pdf (11.07.2016).

38 Vgl. Department of Homeland Security: Assessing ISIL's Influence and Perceived Legitimacy in the Homeland. A State and Local Perspective. Field Analysis Report, Mai 2015, S. 6.

39 Vgl. Berger, „The Evolution of Terrorist Propaganda. The Paris Attack and Social Media".

40 Vgl. Berger, J.M./Perez, Heather: The Islamic State's Diminishing Returns on Twitter. How suspensions are limiting the social networks of English-speaking ISIS supporters. George Washington University Program on Extremism Occasional Paper, Februar 2016, S. 6.

41 Vgl. Wittich, Elke: „Tweets aus dem Jihad", Jungle World online, 19.02.2015, http://jungle-world.com/artikel/2015/08/51470.html, (19.07.2016).

und -Kämpfern erfolgen. Ebenfalls können GPS-Koordinaten von Terroristen und deren Verstecken gewonnen werden.[42] Dies hat einen weiterführenden Effekt: Können GPS-Koordinaten eines ausländisches IS-Kämpfers, der sich der Terrororganisation in Syrien oder dem Irak angeschlossen hat, abgegriffen werden, ermöglicht dies nach einer eventuellen Rückkehr in seine Heimat eine Strafverfolgung, da anhand der GPS-Koordinaten bewiesen werden kann, dass er sich zeitweise im Territorium des IS aufhielt.[43] Da Twitter-Accounts somit eine wichtige Informationsquelle für eine spätere Verurteilung von IS-Mitgliedern und -Anführern darstellen, sollten solche Informationen als Beweismaterial für Kriegsverbrechen und die Verletzung von Menschenrechten gesammelt werden, bevor eine Suspendierung der Accounts erfolgt.[44] Zudem ist es nicht nur für Behörden interessant, einige Accounts bestehen zu lassen; auch für Wissenschaftler, die anhand dieser Profile ihre Forschung vorantreiben können, ist es von Interesse.

Gegen eine Deaktivierung spricht weiterhin, dass suspendierte Accounts keinen Raum für ein mögliches Countertweeting im Rahmen von Public Diplomacy-Maßnahmen lassen. Solche Countertweets haben, wenn korrekt eingesetzt, eventuell einen größeren Effekt, als das bloße Suspendieren eines Accounts, auch wenn hierbei angemerkt werden muss, dass bisher keine Erhebungen über den Erfolg von solchen Maßnahmen vorliegen.[45]

Auch die Frage der freien Meinungsäußerung muss in dieser Argumentation Beachtung finden, jedoch mehr aufgrund der Tatsache, dass sie vom IS instrumentalisiert werden kann.[46] Ein bloßes Deaktivieren spielt in die Hände des IS, der sich darauf berufen kann, dass „der Westen" keine freie Meinungsäußerung zulasse. Auch spielt Anonymous in die Hände des IS, da das Netzwerk den Eindruck erweckt, im Namen „des Westens" zu handeln, was den Hass auf den Westen verstärken und zu weiteren Anschlägen führen kann.

Weiterhin droht das großangelegte Deaktivieren von Accounts immer auch eine Gegenreaktion des IS hervorzurufen. So kündigte die Terrororganisation als Reaktion auf #OpParis auf Arabisch einen Gegenschlag gegen Anonymous an.[47] Allerdings muss die-

42 Vgl. Berger/Morgan, The ISIS Twitter Census, S. 54.
43 Vgl. Wittich, „Tweets aus dem Jihad".
44 Vgl. Berger, J.M./Stern, Jessica: „A 6-Point Plan to Defeat ISIS in the Propaganda War", Time online, 30.03.2015, http://time.com/3751659/a-6-point-plan-to-defeat-isis-in-the-propaganda-war/, (13.07.2016).
45 Beispiel für eine Countertweeting-Maßnahme wäre z.B. die Initiative Global Engagement, hier mit dem Tweet von @TheGEC, 13.11.2014, https://twitter.com/TheGEC/status/532966458771640320, (13.07.2016).
46 Vgl. Cottee, Simon: „The Cyber Activists Who Want to Shut Down ISIS", The Atlantic online, 08.10.2015, http://www.theatlantic.com/international/archive/2015/10/anonymous-activists-isis-twitter/409312/, (13.07.2016).
47 Eine Wissenschaftlerin der Quilliam Foundation entdeckte die Nachricht: Vgl. Engel, Pamela: „ISIS is taunting Anonymous with a declaration of 'war'", Business Insider online, 19.11.2015, http://

ses Argument relativiert werden: Der IS kündigte zwar eine Gegenreaktion an, tatsächliche Anschläge oder eine Hackattacke des IS gegen Anonymous blieben aber aus.

Ein wichtiges Argument, das ebenfalls gegen die Deaktivierungen spricht, findet sich ganz spezifisch im Netzwerk Anonymous selbst. Die Gruppe besteht aus einer unbekannten Anzahl von Hackern, die sich zwar unter dem Namen Anonymous vereinen, aber keiner Struktur oder Hierarchie innerhalb dieses Netzwerkes folgen. So hat Anonymous keinen Sprecher und kann seine Aktionen nur bedingt koordinieren.[48] Dies hat zur Folge, dass bei Account-Suspendierungen die Trefferquote zu wünschen übrig lässt. Es wird immer wieder bemängelt, dass suspendierte Accounts zuvor nur unzureichend geprüft worden seien und sich daher auf diversen Listen Namen von Accounts finden, die von Journalisten oder Wissenschaftlern genutzt werden. Auch wissenschaftliche Plattformen wie Jihadica oder Jihadology wurden bereits zum Ziel von Suspendierungen durch Anonymous.[49]

4. Evaluation sowie alternative Akteure und Handlungsoptionen

Auch wenn festzustellen ist, dass die Account-Deaktivierungen generell und auf lange Sicht Erfolg haben,[50] sprechen nicht wenige Argumente gegen die Suspendierung von Twitter-Accounts, zumindest gegen eine Suspendierung, wie sie von Anonymous betrieben wird.

Auch in Zukunft wird es wohl nicht zu koordinierteren Deaktivierungen kommen, da Anonymous ganz bewusst eine dezentrale Herangehensweise fördert. So veröffentlichte die Gruppe „Hack-Anleitungen" für jegliche Personen, die sich an der Bekämpfung der IS-Propaganda beteiligen möchten. Diese Anleitungen sind online zugänglich und erläutern, wie man beispielsweise Twitter-Accounts aufspürt, die mit dem IS affiliiert sind;[51] weitere Seiten, die jedoch bereits gesperrt wurden, erläuterten, wie man diese Accounts schließlich hackt.[52]

Wie könnte dagegen ein koordinierteres Vorgehen aussehen? Aus Ermangelung an Wissen darüber, wie Nachrichten- und Geheimdienste in diesem Feld tatsächlich agieren, muss im

www.businessinsider.com.au/isis-anonymous-statement-2015-11?r=US&IR=T, (13.07.2016).

48 Da die geläufige Anonymous-Website momentan nicht zu aufzurufen ist (http://anonnews.org/?p=press&a=item&i=31, 13.07.2016), wurden diese Informationen hier entnommen: Vgl. Kelly, Brian B.: „Investing in a Centralized Cybersecurity Infrastructure. Why 'Hacktivism' can and should Influence Cybersecurity Reform", in: Boston University Law Review, Vol. 92, S. 1664–1711, S. 1678f.

49 Ein Beispiel für eine solche Liste ist: „OPISIS", Pastebin, 04.01.2016, http://pastebin.com/dhGjZBkx, (11.07.2016); in diesem Tweet forderte der Wissenschaftler Aaron Zelin die Hackergruppen auf, die Attacken gegen seine Webseite Jihadology einzustellen, die im Rahmen der #OpParis erfolgt waren: @azelin, 23.11.2015, https://twitter.com/azelin/status/668805717491589120?ref_src=twsrc%5 Etfw, (12.07.2016).

50 Vgl. Berger/Morgan, The ISIS Twitter Census, S. 55.

51 Die Anleitung findet sich hier: „Instructions", Ghostbin, ohne Datum, https://ghostbin.com/paste/vt5zz, (12.07.2016).

52 Bereits gesperrt wurde diese Ghostbin-Seite: https://ghostbin.com/paste/jrr89, (12.07.2016).

Kontext dieser Fallstudie auf die Arbeit einer Hackergruppe, die quasi-nachrichtendienstliche Informationsbeschaffung vornimmt, zurückgegriffen werden. Aus Anonymous heraus entstand ein weiteres Netzwerk, das eine etwas andere Strategie verfolgt. Die sogenannte „Ghost Security Group" (GSG), die sich selbst als Counterterrorismus-Organisation bezeichnet,[53] distanzierte sich in einer Pressemitteilung im Dezember 2015 von Anonymous und seiner Vorgehensweise.[54] Die Gruppe besteht nach eigenen Angaben aus elf erfahrenen Experten[55], die unter anderem soziale Medien, Mailverkehr und Websites überwachen, Datenanalyse vornehmen sowie Kryptowährungen verfolgen, um Finanzströme von Terrornetzwerken offen zu legen. Außerdem betreiben sie Gefahrenanalyse und behaupten von sich, anhand gesammelter Daten Personenprofile erstellen zu können.[56]

Bei ihrer Vorgehensweise ist die GSG auf Tipps von Usern angewiesen. Angeblich erhält die Gruppe etwa 500 Hinweise pro Tag und startet aufgrund dieser einen strengen Überprüfungsprozess, in den auch arabische Muttersprachler involviert sind. Stellt sich nach einer solchen Überprüfung heraus, dass ein Account oder Websites mit dem IS affiliert sind, schlägt die GSG diese für eine Suspendierung vor und veröffentlicht auf Twitter Listen mit den Namen von betroffenen Accounts oder Websites. Zudem sammelt die Gruppe IP-Adressen verdächtiger Geräte sowie Standortkoordinaten und schleust auch „Online-Spione" in Foren ein, wo sie IS-Unterstützer ausspionieren sollen. Gesammelte Informationen werden dann über Dritte an staatliche Stellen herangetragen.[57]

Somit grenzt sich die GSG nicht nur durch ihre Kooperation mit Behörden von Anonymous ab, auch hat die Gruppe im Gegensatz zu Anonymous eine Struktur sowie Hierarchie und kann ihr Vorgehen besser koordinieren.[58] Die GSG bemängelt zudem, dass Anonymous keinerlei Erfahrung in Terrorismusbekämpfung habe und dass die Vorgehensweise des Netzwerkes – das bloße Deaktivieren von Accounts – bei der Bekämpfung des IS eher hinderlich sei. Die GSG bevorzuge es, wenn Anonymous Accounts nicht so rigoros suspendiere, da somit weiterhin Informationen für Geheimdienste gesammelt werden kön-

53 Vgl. Ghost Security Group: Ohne Titel. Website der Ghost Security Group, ohne Datum, https://ghostsecuritygroup.com, (12.07.2016).
54 Vgl. dazu die Pressemitteilung: Ghost Security Group: „Official Press Release", Archive online, ohne Datum, https://archive.org/stream/GhostSecurityGroupOfficialPressRelease/Ghost%20Security%20Group%20Official%20Press%20Release#page/n1/mode/2up, (12.07.2016).
55 Vgl. Ghost Security Group: „Operatives", Website der Ghost Security Group, ohne Datum, https://ghostsecuritygroup.com/operatives/, (20.07.2016).
56 Vgl. Ghost Security Group: „Capabilities", Website der Ghost Security Group, ohne Datum, https://ghostsecuritygroup.com/capabilities/, (12.07.2016).
57 Vgl. Brooking, E.T.: „Anonymous vs. The Islamic State", Foreign Policy online, ohne Datum, https://foreignpolicy.com/2015/11/13/anonymous-hackers-islamic-state-isis-chan-online-war/, (13.07.2016).
58 Vgl. Ghost Security Group, „Operatives".

nen, wie es der Geschäftsführer der GSG in einem BBC-Interview erläuterte.[59] Die GSG nimmt für sich in Anspruch, mittels dieser Vorgehensweise bereits erste Erfolge verzeichnen zu können: Mit ihrer Arbeit habe die Gruppe dazu beigetragen, einen geplanten Anschlag in Tunesien zu vereiteln. Allerdings wurden diese Zusammenhänge nie vom FBI bestätigt, ihnen wurde aber auch nie widersprochen.[60]

5. Schlussteil und Handlungsempfehlung

Es hat sich gezeigt, dass Deaktivierungen im Allgemeinen nicht als „Allheilmittel" im Kampf gegen die IS-Online-Propaganda angesehen werden können. Werden sie dennoch vorgenommen, sollten sich die Suspendierungen auch auf andere soziale Medien erstrecken, anstatt sich nicht nur auf Twitter zu fokussieren, da angenommen werden kann, dass der radikalere Kreis der Terroristen weniger populäre, dafür aber auch weniger strikt überwachte Plattformen nutzt.

Vielmehr hat sich jedoch gezeigt, dass die eigentliche Problematik des Deaktivierens nicht im Suspendieren von Accounts selbst liegt, sondern in der Zielaufklärung und -auswahl. Für wirklich effektive Suspendierungen bedarf es genauer Kenntnisse über die Swarmcast-Struktur des IS-Netzwerkes, und anschließend relativ kurzer, aber umso konzentrierterer Aktionen, um signifikante Teile des Netzwerks, anstatt nur einzelner, austauschbarer Verbindungsglieder, auszuschalten.

Darüber hinaus sollte bedacht werden, dass vor Deaktivierungen Daten aus Accounts abgeschöpft werden können, die beim Vorgehen gegen den physischen IS hilfreich sein können – evtl. bis hin zur Anschlagsvereitelung. Ein Netzwerk wie Anonymous, das generell die Kooperation mit staatlichen Stellen verweigert, lässt diese Möglichkeiten ungenutzt.

Deaktivierungen von Social Media-Accounts können also im Kampf gegen die IS-Online-Propaganda durchaus von großem Nutzen sein, wenn sie sinnvoll koordiniert sind und eine Weiterleitung von Informationen, die von gehackten und später deaktivierten Accounts abgegriffen wurden, an entsprechende staatliche Stellen nicht ausschließen. Hierfür ist die Arbeit der Ghost Security Group – auch wenn sie nicht unkritisch beobachtet werden darf – ein Beispiel.

59 Vgl. Wendling, Mike: „Ghost Security Group 'Spying' on Islamic State instead of hacking them", BBC online, 23.11.2015, http://www.bbc.com/news/blogs-trending-348799 90, (13.07.2016).
60 Vgl. Brooking, „Anonymous vs. The Islamic State".