Gesellschaftliche Herausforderungen des Missbrauchs von Bots und sozialen Medien

Marc-André Kaufhold, Christian Reuter, Marvin Stefan

Institut für Wirtschaftsinformatik, Universität Siegen

Zusammenfassung

Soziale Medien wie Facebook oder Twitter haben sich als alltägliche Kommunikationskanäle etabliert. Aufgrund der großen Reichweite sind diese Medien für den privaten oder öffentlichen Austausch unter Freunden und Gruppierungen sowie zur Produkt- und Unternehmenswerbung geeignet, unterliegen aber auch der Gefahr der Manipulation öffentlicher Diskurse oder des Missbrauchs der jeweiligen Plattformfunktionen. Hierzu werden unter anderem Bots, und spezifischer „Social Bots“, als automatisierte Programme eingesetzt, um einen Einfluss auf ökonomische, politische und soziale Prozesse auszuüben. Dieser Beitrag stellt die vorläufigen Ergebnisse einer systematischen Literaturstudie und thematischen Analyse dar, welche gesellschaftliche Herausforderungen sowie zugehörige Methoden und Vorgehensweisen des Missbrauchs von Bots und sozialen Medien umfassen.

1 Einleitung

Soziale Netzwerke (Online Social Networks, kurz: OSN) wie Facebook oder Twitter sind in den letzten Jahren nicht nur im persönlichen Alltag, sondern auch in sicherheitskritischen Kontexten (z.B. Notfälle, Katastrophen) und im öffentlich-politischen Diskurs immer populärer geworden (Reuter & Kaufhold, 2018). Durch die häufige Nutzung und die vielen Benutzer können dort geteilte Inhalte eine große Reichweite generieren. Sie sind daher beliebte Plattformen, um für sich oder eine Organisation zu werben und sich zu aktuellen, politischen und sozialen Themen zu äußern.

Aus diesem Grund werden sie auch von vielen Aktivisten und politischen Akteuren verwendet (Diamond, 2010). Ihre Handlungen in den Netzwerken beschränken sich dabei allerdings nicht notwendiger Weise auf die vorgesehene Nutzung, sondern auch auf den Missbrauch der Plattformen, wodurch menschengemachte Beeinträchtigungen des öffentlichen Lebens und Notsi-

Veröffentlicht durch die Gesellschaft für Informatik e.V. 2017 in
M. Burghardt, R. Wimmer, C. Wolff, C. Womser-Hacker (Hrsg.):
Mensch und Computer 2017 - Workshopband, 10.-13. September 2017, Regensburg.
 https://doi.org/10.18420/muc2017-ws01-0386

tuationen etwa durch Massenhysterien und Panik entstehen können (Ferrara, 2015). Sie werden zum Beispiel zur Manipulation von Wahlen oder für andere politische Angelegenheiten ausgenutzt, indem Desinformationen und Propaganda verbreitet werden (Reuter, Pätsch, & Runft, 2017). Zur Manipulation werden einfache Maßnahmen, wie das Verbreiten von Propaganda in Form von Nachrichten, Bildern und Videos, oder auch aufwendige, wie das Umleiten zu pseudo-oppositionellen Seiten oder das Engagieren von bezahlten Kommentatoren, umgesetzt (Doll, 2011).

Die Verbreitung erfolgt durch reguläre Benutzerprofile oder durch den Einsatz von Bots oder organisierten Bot-Netzen. Dabei sind Bots in OSN teil- oder vollautomatische Programme, die ein Benutzerprofil steuern können und etwa zum Spam von Nachrichten, zum Retweeten (auf Twitter) oder zum Posten von Inhalten anderer Webseiten verwendet werden. Damit die für diesen Missbrauch verwendeten Bots nicht einfach als solche identifiziert werden können, werden sie so programmiert und verwaltet, dass sie das Verhalten echter Menschen imitieren. Diese *Social Bots* werden mitunter genutzt, um politische Diskurse zu infiltrieren, den Aktienmarkt oder betriebliche Prognosen zu manipulieren, persönliche Informationen zu stehlen, Fehlinformationen zu verbreiten oder die persönliche Wahrnehmung (z.B. durch Spam) zu beeinflussen (Ferrara, Varol, Davis, Menczer, & Flammini, 2016). Mit der Verbreitung von Propaganda sollen beispielsweise Wähler beeinflusst werden, die sich erst kurz vor der Wahl für eine der Wahloptionen entscheiden. Die Inhalte, die von Bots gepostet werden, üben nicht nur auf ihre Adressaten Einfluss aus, sondern erschweren zusätzlich das Durchführen von Studien über OSN, da authentisch geführte Social Bots kaum von echten Benutzern zu unterscheiden sind (Hegelich, 2016). Plattformen wie Facebook und Twitter verfügen zwar über Software zur Erkennung von Bots, aber diese sind noch nicht in der Lage, alle Bots zu identifizieren. Zusätzlich können Bot-Netze die Erkennung teilweise umgehen, da meist nur einzelne Bots erkannt werden (Zhang, Zhang, Zhang, & Yan, 2013).

Auch außerhalb von OSN werden Bots für gesellschaftliche und politische Zwecke eingesetzt. Hier werden meist PCs genutzt, sogenannte *Zombies*, die mit Malware infiziert sind und über diese ferngesteuert werden können. Die Zombies werden zu Bot-Netzen vereinigt, um unter anderem Denial-of-Service-Angriffe (DoS) auszuführen oder Passwörter mit der Brute-Force-Methode zu ermitteln. Durch DoS- oder Distributed-Denial-of-Service-Angriffe (DDoS) können hohe finanzielle oder Reputationsschäden bei den Opfern entstehen sowie politische Konflikte motiviert werden (Landler, 2007), etwa wenn durch Cyberangriffe virtuelle oder physische Infrastrukturen gezielt beeinträchtigt werden (Gandhi et al., 2011).

Das Ziel der systematischen Literaturstudie und thematischen Analyse ist es, gesellschaftliche Herausforderungen des Missbrauchs von Bots und sozialen Medien zu untersuchen. In dieser Workshoppublikation werden vorläufige Ergebnisse der noch laufenden Studie präsentiert. Dazu werden zunächst die Methodik der systematischen Literaturstudie (Kapitel 2) und die vorläufigen Ergebnisse einer darauf basierenden thematischen Analyse (Kapitel 3) vorgestellt. Diese umfassen die Betrachtung der identifizierten Themen (1) Identitätsdiebstahl, (2) fiktive Initiativen, (3) Cyberangriffe, (4) Reichweitenmanipulation, (5) Wahrnehmungsbeeinflussung sowie (6) extremistische Propaganda und Rekrutierung. Der Beitrag schließt mit einem Zwischenfazit ab (Kapitel 4).

2 Methodik der Literaturstudie

In dieser systematischen Literaturrecherche (Paré, Trudel, Jaana, & Kitsiou, 2015) werden gesellschaftliche Herausforderungen des Missbrauchs von Bots und sozialen Netzwerken untersucht. Die erste Recherche erfolgte nicht systematisch über Google Scholar. Dabei wurden 25 relevante Quellen gefunden, auf deren Basis der folgende Suchbegriff mit drei Segmenten für die systematische Literaturrecherche gebildet wurde:

((politic OR terror* AND ("bot" OR "botnet" OR "social media" OR "social network")) AND ("false flag" OR manipulation OR propaganda OR sybil OR hack* OR "cyber attack" OR "disinformation" OR "misinformation" OR disrupt* OR spam*)) OR ((("social network" OR "social media") AND ("bot" OR "botnet") AND (sybil OR "disinformation" OR "misinformation" OR spam* OR "detection" OR hack*)) OR astroturf* OR crowdturf*)*

Das erste Segment fokussiert den politischen Missbrauch von Bots und OSN, das zweite Segment (unterstrichen hervorgehoben) konzentriert sich allgemein auf die bösartige Verwendung von Bots und OSN. Das letzte Segment befasst sich ausschließlich mit Astroturfing und Crowdturfing, da diese Begriffe einzeln bessere Funde lieferten als in Verbindung mit anderen.

Datenbank	**Gesamtzahl**	**Titel**	**Abstract**	**Volltext**
ACM DL	37	34	30	15
IEEE Xplore	204	72	65	38
JSTOR	262	13	13	7
ScienceDirect	39	16	15	8
SpringerLink	204	28	25	18
Summe	*746*	*163*	*149*	*86*

Tabelle 1. Datenbanken mit Gesamtresultaten und Filterung nach Titel, Abstract und Volltext

Die systematische Literaturrecherche wurde auf fünf Datenbanken angewandt (Tabelle 1). Unter Berücksichtigung von Quellen, die nach 2007 erschienen sind, wurden insgesamt 746 Suchergebnisse in allen Datenbanken gefunden, die nach der Titelfilterung auf 163 reduziert wurden. Wenn anhand des Titels im Hinblick auf Kriterium (1) (s.u.) keine Einschätzung über die Relevanz getroffen werden konnte, wurden in einzelnen Fällen bereits die Abstracts hinzugezogen. Die verbleibenden Quellen wurden anschließend auf ihre Relevanz über das Abstract oder den Volltext nach fünf Kriterien evaluiert, die zur Restsumme von 86 Quellen führten:

1) Weder Bots, soziale Medien noch Gesellschaft oder Politik wurden thematisiert.
2) Bots wurden thematisiert, aber in keinen ges. oder pol. Kontext gesetzt.
3) Ein ges. oder pol. Kontext wurde ohne Bezug zu Bots oder OSN motiviert.
4) Die Quelle stellt keinen Bezug zum Missbrauch von Bots oder OSN her.
5) Die Quelle enthält nur wenig relevante Informationen.

Bei der Überprüfung nach Abstract und Volltext wurden zunächst Regel (1) und, sofern diese nicht zutraf, je nach Inhalt des Papers einige der Regeln (2) bis (4) angewandt. Wenn keine dieser Regeln zum Ausschluss der Quelle führte, wurde abschließend Regel (5) überprüft.

3 Vorläufige Ergebnisse der thematischen Analyse

Die vorläufigen Ergebnisse wurden im Rahmen der thematischen Analyse in sechs Themenbereiche zum gesellschaftlichen Missbrauch gruppiert, die im Folgenden kurz vorgestellt werden.

3.1 Identitätsdiebstahl mit Account Hijacking

Accounts, die temporär oder vollständig durch *Account Hijacking* von Angreifern übernommen wurden, nennt man kompromittierte Accounts. Die menschlichen Angreifer oder programmierte Bots gelangen zum Beispiel durch Phishing, Malware oder Cross-Site-Scripting an die Anmeldedaten eines Benutzers. Eine häufig von den Angreifern angewandte Phishing-Technik ist es, über bereits kompromittierte Accounts weitere Angriffe zu starten. Sie versuchen das Vertrauen der befreundeten User zu missbrauchen (Stein, Chen, & Mangla, 2011). Bei Malware-Angriffen wird Schadsoftware benutzt, um die Anmeldedaten zu stehlen oder die User-Session zu übernehmen (Stein et al., 2011). Malware kann sich selbst replizieren, wenn sie als Form von Viren vorhanden ist, indem sie Links oder direkte Downloads an andere OSN-Benutzer schicken. Account Hijacking wird auch für politische Zwecke eingesetzt. Kompromittierte Accounts sind wertvoller als Bots für das Verbreiten von Desinformationen oder Propaganda, da diese bereits Vertrauen zu legitimen Nutzern etabliert haben (Trang, Johansson, & Rosell, 2015). Zusätzlich steigt der Nutzen eines übernommenen Profils, wenn dieser rechtmäßig einer populären Person oder Organisation gehört hat, da den Angreifern durch diese eine enorme Reichweite zur Verfügung steht. Eines der bekanntesten Beispiele für solch einen Vorfall ist die Übernahme des Twitter Accounts der Associated Press, da sich als Folge dieser Nachricht eine große Instabilität des Finanzmarktes ergab (Trang et al., 2015).

3.2 Fiktive Initiativen mit Astro- und Crowdturfing

Astroturfing bezeichnet das Vortäuschen von Graswurzelbewegungen, also lokale, politische oder gesellschaftliche Initiativen oder Organisationen, welche Einfluss auf eine kommerzielle oder politische Situation bzw. einen Zustand ausüben möchten (Cho et al., 2017). Politisches Astroturfing wird meist unter Zuhilfenahme von Bots genutzt, um unabhängige Meinungsäußerungen vorzutäuschen, die tatsächlich aber von politischen Gruppen in Auftrag gegeben wurden. Sie werden weiterhin eingesetzt, um eigene Argumente zu unterstützen sowie Gegenargumente anzuzweifeln oder zu leugnen, und dadurch die Auffassungen und Sichtweisen der Bevölkerung zu manipulieren (Cho et al., 2017). Dabei werden oft illegale oder Grauzoneninhalte verbreitet, wie z.B. Werbebetrug, fragwürdige politische Aussagen oder rufschädigende Gerüchte (Wang et al., 2012). In OSN werden die gefälschten Meinungsäußerungen entweder durch Bots oder von bezahlten Autoren verbreitet. Astroturfing findet auch außerhalb von OSN statt und wurde z.B. für Argumente gegen die globale Erwärmung eingesetzt (Cho et al., 2017). Der Begriff *Crowdturfing* setzt sich aus „Crowdsourcing“ und „Astroturfing“ zusammen und ist eine Variante, bei der Gruppen von Menschen Astroturfing durchführen. Der Einsatz dieser Gruppierungen hat gegenüber von Bots den Vorteil, dass konventionelle Identifikationsverfahren von bösartigen Aktivitäten, die darauf beruhen, Bots zu erkennen, umgangen

werden können (Song, Lee, & Kim, 2015). Die Identifikation wird zusätzlich dadurch erschwert, dass die Arbeiter ihre Accounts ebenso für normale Tätigkeiten gebrauchen und in einem flexiblen bzw. ohne einen Zeitplan arbeiten, wodurch sie schwieriger von normalen Benutzern zu unterscheiden sind (Song et al., 2015).

3.3 Cyberangriffe am Beispiel von Bot-Netzen

Cyberangriffe, die mit Zombies bzw. Bot-Netzen aus Zombierechnern ausgeführt werden, sind in den meisten Fällen DoS-Angriffe. Diese können die virtuelle und, insbesondere bei enger Verzahnung, physische Infrastruktur beeinträchtigen, etwa Banken, das Gesundheitswesen oder die Stromversorgung (Gandhi et al., 2011). Ein bekanntes Beispiel für einen solchen Angriff ist der DDoS-Angriff auf Estland (2007), wobei sowohl Webseiten des estländischen Parlaments, des Präsidenten und der Regierungsbehörden als auch Webseiten der zwei größten estländischen Banken und Nachrichtenseiten nicht mehr verfügbar waren (Hansen & Nissenbaum, 2009). Der Angriff hat über drei Wochen angedauert und es wurden weltweit etwa eine Millionen Zombies für ihn verwendet, doch die Täter konnten nicht identifiziert werden (Gandhi et al., 2011). Bei einem weiteren Cyberangriff, der 2008 in einem Konflikt zwischen Russland und Georgien herrschte, konnten ebenso keine sicheren Aussagen über den Täter gemacht werden, obwohl später ein Bot-Netz-Provider gefunden wurde, der für die Angriffe mitverantwortlich war (Gandhi et al., 2011). Die Beispiele zeigen, dass die Identifikation der Ausführenden von Cyberangriffen ein großes Problem darstellt, da die Täter keine Konsequenzen für ihr Handeln tragen müssen. Selbst wenn ein Staat klare Beweise für die Überführung des Ausführers eines Angriffs ermittelt hat, gibt es keine Definition, welche Arten und Weisen von Cyberangriffen einen Kriegsakt darstellen (Applegate, 2011).

3.4 Reichweitenmanipulation durch Fake Follower und Retweets

Fake Follower und Fake Retweets – im Beispiel des OSN Twitter – werden eingesetzt, um Popularität vorzutäuschen (Jiang, Cui, Beutel, Faloutsos, & Yang, 2016; Wu, Fan, Gao, Feng, & Yu, 2015). Durch das Folgen einer Person auf Twitter erscheinen dessen Tweets und Retweets auf der eigenen Startseite. Daher werden Accounts mit vielen Followern als populärer und einflussreicher angesehen. Es gibt Politiker und berühmte Persönlichkeiten, die sich durch den Kauf von *Fake Followern* eine statistisch größere Popularität verschaffen oder ihren Wert auf Twitter erhöhen möchten (Jiang, Cui, Beutel, Faloutsos, & Yang, 2016). Beispielsweise werden Persönlichkeiten mit einer größeren Anzahl an Accounts, die ihnen folgen, mit einem größeren sozialen Einflussreichtum, durch ihre hohe Reichweite, assoziiert und sind dadurch interessanter für Werbepartner (Wu, Fan, Gao, Feng, & Yu, 2015). Durch *Fake Retweets* wird die künstliche Popularität einer Nachricht vorgetäuscht (Wu, Fan, Gao, Feng, & Yu, 2015). Die tatsächliche Zahl an Personen, die diese Nachricht erreicht, muss mit den zusätzlichen falschen Retweets aber nicht steigen, es sei denn die Accounts, mit denen der Betrug ausgeführt wird, besitzen selber auch legitime Follower. Künstliche Retweets und Follower werden meist auf Online-Marktplätzen gekauft. Ausgeführt wird der Betrug mit Hilfe von Bot-Accounts oder Malware-infizierten Accounts.

3.5 Wahrnehmungsbeeinflussung durch Spam

Spam, in OSN auch *Social Spam*, wird beispielswiese zur Verbreitung von Malware- (Infektion und Fernsteuerung von Zombie-Bots) oder Phishing-infizierten Seiten (Account-Diebstahl) benutzt (Almaatouq et al., 2016). Aus politischen Gründen wird es dagegen gebraucht, um die öffentliche Meinung zu beeinflussen, falsche oder irreführende Informationen zu verbreiten oder Kommunikation von Benutzern zu verhindern bzw. zu erschweren (z.B. die Kommunikation über ein aktuelles politisches Ereignis). Ein Ziel von Spam besteht darin, die Wahrnehmung der OSN-Benutzer zu einem bestimmten Thema zu beeinflussen. Mit *Misdirection* wird versucht, von einem Thema auf ein anderes abzulenken, indem Posts zu einem Hashtag gespammt werden, die andere Ereignisse thematisieren, die nicht im Kontext zu dem eigentlichen Thema stehen. Zum Beispiel wurde ein syrisches Bot-Netz verwendet, welches Tweets zu verschiedenen Ereignissen in anderen Teilen der Welt verbreitete, die in keinem Zusammenhang mit dem verwendeten Hashtag standen (Abokhodair, Yoo, & McDonald, 2015). Beim *Smoke Screening* hingegen, werden Nachrichten zu einem Thema bzw. Hashtag verbreitet, um relevante Posts zu einem Thema durch die große Anzahl anderer Posts schwieriger auffindbar zu machen. Diese Taktik wurde auch von syrischen Bots angewendet, um Nachrichten zum Hashtag „#Syria“, die positiv für die Revolution gestimmt waren, zu überhäufen (Abokhodair et al., 2015).

3.6 Propaganda und Rekrutierung am Beispiel des Terrorismus

OSN werden z.B. von Terrororganisationen genutzt, um *Propaganda* zu verbreiten und neue Mitglieder zu rekrutieren. Außerdem können sie dadurch die traditionellen Medien umgehen, um zu garantieren, dass Botschaften unverändert ankommen (Weimann, 2015). Vor der Nutzung von OSN sind Terroristen größtenteils in selbsterstellten Foren tätig gewesen. Diese sind sicherer vor unerwünschten Eindringlingen, allerdings auch weniger erreichbar für potenzielle neue Rekruten oder Sympathisanten (Torok, 2013). So können Terroristen auf OSN aktiv nach potenziellen Mitgliedern suchen, um diese in die eigenen Foren zu locken (Weimann, 2015). Selbsterstellte Webseiten werden für das Trainieren und Rekrutieren von neuen Mitgliedern, das Vergrößern von Geldmitteln, zur Kommunikation sowie zum Planen und Starten von Angriffen verwendet (Weimann, 2015). Inzwischen werden auch Social Bots von Terrororganisationen genutzt. ISIS hat Social Bots für Propaganda und Rekrutierungen eingesetzt, welche je nach ihrer Zielgruppe verschiedene Manipulationsstrategien anwenden können (Ferrara, 2015). Terrororganisationen verwenden YouTube aufgrund der einfachen Zugänglichkeit für die Verbreitung von Propaganda und Radikalisierungsvideos (Weimann, 2015). Andere Inhalte, die auf Twitter geteilt werden, sind Propaganda, Aufrufe zum Handeln, Instruktionen für die Ausführung von Taten sowie Nachrichten von Anschlägen und Kämpfen (Weimann, 2015). Weiterhin wird auch Facebook dafür genutzt, um Propaganda und Instruktionen weiterzuleiten. Dazu zählen z.B. taktische Informationen, Baupläne für Bomben oder Gebrauchsanleitungen für Waffen und deren Wartung (Weimann, 2015).

4 Zwischenfazit

Dieser Beitrag hat die vorläufigen Ergebnisse einer systematischen Literaturstudie und thematischen Analyse dargestellt, mit dem Ziel, gesellschaftliche Herausforderungen des Missbrauchs von Bots und sozialen Medien zu untersuchen. Dazu wurden die Phänomene (1) Identitätsdiebstahl, (2) fiktive Initiativen, (3) Cyberangriffe, (4) Reichweitenmanipulation, (5) Wahrnehmungsbeeinflussung, sowie (6) extremistische Propaganda und Rekrutierung vorgestellt. Die präsentierten Ergebnisse befinden sich in einem frühen Stadium und bedürfen einer iterativen, vertiefenden Analyse, um robuste und systematische Kategorisierungen, Methoden, Themen und Vorgehensweisen zu entwickeln. Da der Missbrauch von Bots und sozialen Medien, direkt oder indirekt, infrastrukturelle, gesellschaftliche, persönliche, politische und ökonomische Schäden verursachen kann, erscheint es relevant, deren Gefahren und Umfang zu dokumentieren sowie wirksame Gegenmaßnahmen zu entwickeln, die sich etwa durch netzwerkbasierte Techniken, Crowdsourcing-Strategien, überwachtes maschinelles Lernen und hybride Systeme realisieren lassen (Ferrara et al., 2016).

Literaturverzeichnis

Abokhodair, N., Yoo, D., & McDonald, D. W. (2015). Dissecting a Social Botnet. *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing - CSCW '15*, 839–851.

Almaatouq, A., Shmueli, E., Nouh, M., Alabdulkareem, A., Singh, V. K., Alsaleh, M., … Pentland, A. (2016). If it looks like a spammer and behaves like a spammer, it must be a spammer: analysis and detection of microblogging spam accounts. *International Journal of Information Security*, *15*(5), 475–491.

Applegate, S. (2011). Cybermilitias and Political Hackers: Use of Irregular Forces in Cyberwarfare. *IEEE Security & Privacy*, *9*(5).

Cho, C. H., Martens, M. L., Kim, H., Rodrigue, M., Journal, S., December, N., … Rodrigue, M. (2017). Astroturfing Global Warming : It Isn't Always Greener on the Other Side of the Fence. *Journal of Business Ethics*, *104*(4), 571–587.

Diamond, L. (2010). Liberation Technology. *Journal of Democracy*, *21*(3), 69–83. https://doi.org/10.1353/jod.0.0190

Doll, M. (2011). Revolution 2.0? Über den Zusammenhang zwischen den Aufständen im ›arabischen Raum‹ und ihren medialen Bedingungen. *kultuRRevolution. Zeitschrift Für Angewandte Diskurstheorie*, (H. 60), 64–71.

Ferrara, E. (2015). Manipulation and abuse on social media. *ACM SIGWEB Newsletter*, (Spring), 1–9. https://doi.org/10.1145/2749279.2749283

Ferrara, E., Varol, O., Davis, C., Menczer, F., & Flammini, A. (2016). The Rise of Social Bots. *Communications of the ACM*, *59*(7), 96–104.

Gandhi, R., Sharma, A., Mahoney, W., Sousan, W., Zhu, Q., & Laplante, P. (2011). Dimensions of Cyber-Attacks. *IEEE Technology and Society Magazine*, 28–38.

Hansen, L., & Nissenbaum, H. (2009). Digital disaster, cyber security, and the copenhagen school. *International Studies Quarterly*, *53*(4), 1155–1175.

Hegelich, S. (2016). Invasion der Meinungs-Roboter. *Analysen Und Argumente, Konrad-Adenauer-Stiftung*, *221*(221), 2–9.

Jiang, M., Cui, P., Beutel, A., Faloutsos, C., & Yang, S. (2016). Catching Synchronized Behaviors in Large Networks: A Graph Mining Approach. *ACM Trans. Knowl. Discov. Data*, *10*(4), 35:1-35:27.

Landler, M. (2007). Digital fears emerge after data siege in Estonia. *New York Times*, 1–5.

Paré, G., Trudel, M. C., Jaana, M., & Kitsiou, S. (2015). Synthesizing information systems knowledge: A typology of literature reviews. *Information and Management*, *52*(2), 183–199.

Reuter, C., & Kaufhold, M.-A. (2018). Fifteen Years of Social Media in Emergencies: A Retrospective Review and Future Directions for Crisis Informatics. *Journal of Contingencies and Crisis Management (JCCM)*, *26*(1).

Reuter, C., Pätsch, K., & Runft, E. (2017). Terrorbekämpfung mithilfe sozialer Medien – ein explorativer Einblick am Beispiel von Twitter. In *Proceedings of the International Conference on Wirtschaftsinformatik (WI)*. St. Gallen, Switzerland.

Song, J., Lee, S., & Kim, J. (2015). CrowdTarget. *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security - CCS '15*, (i), 793–804.

Stein, T., Chen, E., & Mangla, K. (2011). Facebook immune system. *Proceedings of the 4th Workshop on Social Network Systems*, *m*(5), 1–8.

Torok, R. (2013). Developing an explanatory model for the process of online radicalisation and terrorism. *Security Informatics*, *2*(6), 1–10.

Trang, D., Johansson, F., & Rosell, M. (2015). Evaluating Algorithms for Detection of Compromised Social Media User Accounts. *Proceedings - 2nd European Network Intelligence Conference, ENIC 2015*, 75–82.

Wang, G., Wilson, C., Zhao, X., Zhu, Y., Mohanlal, M., Zheng, H., & Zhao, B. Y. (2012). Serf and Turf: Crowdturfing for Fun and Profit. *Arxiv Preprint arXiv:1111.5654*, 10.

Weimann, G. (2015). Terror and the Internet. In *International Encyclopedia of the Social & Behavioral Sciences* (pp. 227–236).

Wu, X., Fan, W., Gao, J., Feng, Z. M., & Yu, Y. (2015). Detecting Marionette Microblog Users for Improved Information Credibility. *Journal of Computer Science and Technology*, *30*(5), 1082–1096.

Zhang, J., Zhang, R., Zhang, Y., & Yan, G. (2013). On the impact of social botnets for spam distribution and digital-influence manipulation. *2013 IEEE Conference on Communications and Network Security, CNS 2013*, 46–54.