

Preventing Twitter from Being Used as a Cyberbullying Platform for Defamation, Doxing, and Impersonation

ABSTRACT

The social network Twitter is a sewer of defamation, doxing, and impersonation. Defamation, doxing, and impersonation are three of the major problems of the Internet age and can cause serious damages to victims. This research paper makes recommendations for Twitter policies and public policies to combat online defamation, doxing, and impersonation.

Keywords: Cyberlibel, Cyberbullying, Fake News, Misinformation, Disinformation, Misinformation Identification Engineering

INTRODUCTION

The social network Twitter is infamous for defamation, doxing, and impersonation (Collins, 2011; Cox, 2014; Koch, 2016; Reznik, 2013; Sternberg, 2019). This research paper focuses on combating online defamation, doxing, and impersonation on Twitter. Defamation against an individual involves the communication of false statements that harm the individual's reputation. Doxing of an individual involves the publication of an individual's private information such as his home address or family members. People can be impersonated for many purposes such as to harm their reputations, to gain personal information on them, to cause them to lose business, to cause them to lose friends, to write exams for them, to vote for them, to spread false information about them, etc.

In the old days, it was hard to spread false information or private information about people. It had to be done by telling people face to face, handing out flyers, putting up posters, etc. Only the mainstream media had the means to reach a lot of people. The mainstream media is generally more careful in what it says, although it has crossed the line into defamation many times too, but usually not nearly as bad as people can commit defamation on the world wide web. Now false information or private information about people can just be posted on the web using a fake name

for the world to see (Banerjee & Chua, 2019; Chilwa, 2019; Hage et al., 2020; Pal & Banerjee, 2019; Reynard, 2019; Solo, 2019a, 2019b, 2019c). Defamation, doxing, and impersonation on the web are three of the major new problems of the information age.

Social networks like Facebook and Twitter are frequently used to spread defamatory information. New software can be used to detect cyberbullying on social networks (Balakrishnan et al., 2019). Fake news, which is used to spread disinformation or defamatory information, is a growing problem (Adikpo, 2019; Assay, 2019; Bradshaw & Howard, 2019; Çomlekci, 2020; Dale, 2019; Delellis & Rubin, 2020; Grazulis & Rogers, 2019; Guadagno & Guttieri, 2019; Mach, 2019; Ottonicar, 2020; Rezayi et al., 2018; Stengel, 2019; Watts, 2018). Fake news and defamation on Twitter are frequently used to attack politicians, an unethical type of network politics (Solo & Bishop, 2011, 2014, 2016, 2017). The development of spambots to spread disinformation on politics is an unethical form of political engineering or computational politics (Solo, 2011, 2014, 2017, 2019d). Twitter policies need to be updated as recommended in this research paper to stop defamation, doxing, and impersonation. Also, as recommended in this research paper, laws need to be updated for fighting online defamation, doxing, and impersonation.

Internet defamation, inter alia, severely harms people's reputations; prevents them from getting gainful employment; ruins romantic relationships; causes depression, anxiety, and distress; causes mental health problems, etc. Internet doxing, inter alia, endangers people; causes depression, anxiety, and distress; causes mental health problems; etc. Internet impersonation, inter alia, severely harms people's reputations; prevents them from getting gainful employment; ruins romantic relationships; causes depression, anxiety, and distress; causes mental health problems, etc.

Most private employers these days do web searches on prospective employees to see what turns up. If they have a bunch of people applying for one position, as is usually the case, they aren't going to risk selecting the candidate with a bunch of injurious claims about him on the web whether or not they can determine if it's true.

Humans have a hard time distinguishing between true and false information (Kaufman, 2018; Marsh et al., 2016; Vosoughi et al., 2018). Andrew Butler, an associate professor of psychological and brain sciences at Washington University in St. Louis, said, "Even when people have knowledge that directly contradicts false information, they fail to detect that it is false information (Kaufman, 2018)." Furthermore, humans are predisposed to believing false information. Butler said, "People have a bias to assume truth (Kaufman, 2018)." A research study found that Twitter users are twice as likely to repost fake news as they are to repost real news (Kaufman, 2018; Vosoughi et al., 2018).

The civil remedies for dealing with defamation or doxing are extremely inadequate. Lawyer fees for a defamation or doxing claim in the United States are typically in the range of \$30,000 USD or more. The vast majority of defamation or doxing victims can't afford the legal costs. A civil lawyer with expertise in defamation law said that he got inquiries from a bunch of people defamed on an online hate group, but none could afford to retain him. Most lawyers charge more than this lawyer who has been practicing for a few years. When someone is defamed or doxed on the web, the defamation or doxing typically remains on the Internet until a civil court judgment is obtained and this usually takes years. In the mean time, the victim continues to accumulate all kinds of damages. The author of this research paper has seen people being defamed and doxed on the web

contemplate criminal violence as the only means they have to get the defamation and doxing removed.

Entrepreneur Elon Musk is currently negotiating a purchase of Twitter. He has indicated that he is interested in name authentication for users and protecting freedom of speech. Name authentication is a good idea, but freedom of speech was never meant to protect defamation and has never protected defamation. People don't have the right to go around falsely claiming someone is a prostitute or pedophile, but these are the kinds of false statements that one can regularly see on social networks like Twitter. Musk has been sued for alleged defamation on Twitter (Lee, 2019). He has also complained about alleged false statements against him on Twitter (Holdme, 2022).

RECOMMENDATIONS FOR TWITTER POLICIES

Following are recommendations for responsible Twitter policies to prevent and fight defamation, doxing, and impersonation:

1. Twitter must require users to provide proof of their real names either by providing identification or by making a payment with a credit card or bank card. These websites should not allow anonymous payments with cryptocurrency. This will prevent most cases of defamation, doxing, and impersonation.
2. Twitter must require users to provide proof of their addresses either by providing identification or by making a payment with a credit card or bank card. Users should be required to provide addresses where they can be served with civil claims, subpoenas, search warrants, etc. for content on their profiles. This information may be required by law enforcement or people suing for defamation, doxing, or impersonation and must be turned over with search warrants or subpoenas.
3. Twitter should record the IP addresses of its website users for five years. For each post made on an online forum, Twitter should record the IP address of the individual who made the post and should be required to store this information for five years. This information may be required by law enforcement or people suing for defamation, doxing, or impersonation and must be turned over with search warrants or subpoenas.
4. Twitter should not allow so-called parody profiles because these are frequently used for defamation, doxing, and impersonation. Unknown people made numerous parody accounts on Twitter to attack a mayoral candidate in Regina, Saskatchewan, Canada. These parody accounts had a lot of disinformation on the candidate.
5. Twitter should block search engines from indexing user posts on its website. This can easily be done with a noindex metatag on each webpage with a user post.
6. Twitter should block web archiving systems and search engines from archiving user posts on its website. This can easily be done with noarchive and nosnippet metatags on each webpage with a user post.

7. If someone complains about defamation on Twitter and Twitter system administrators can't verify that it's not defamatory, Twitter system administrators should remove that content.
8. If someone complains about doxing on a Twitter, Twitter system administrators should remove that content.
9. If someone complains about impersonation on Twitter and Twitter doesn't have an identity verification system, then Twitter system administrators should remove that content.

PUBLIC POLICIES FOR FIGHTING ONLINE DEFAMATION, DOXING, AND IMPERSONATION

Laws and public policies need to be updated to deal with online defamation, doxing, and impersonation in the information age. The author of this research paper previously made 12 recommendations for public policies to effectively combat online defamation, doxing, and impersonation (Solo, 2019a; Solo, 2019b; Solo, 2019c; Solo, 2020):

1. Criminal laws for defamation need to be enforced. These laws are rarely enforced in the U.S. and Canada.
2. Defamation should be a criminal offense in every country.
3. Impersonation should be a criminal offense in every country.
4. Online posting of a person's home address without permission should be a crime. This leads people with adversaries to fear for the safety of themselves and their families and their property.
5. Small claims courts must be equipped to deal with defamation, doxing, and impersonation lawsuits and must be able to order preliminary and permanent injunctions. Most victims do not have the expertise for pro se legal representation in higher courts and can't afford the costs of lawyers to represent them in higher courts.
6. Every website owner should be required to record the IP addresses of its website users for five years. For each post made on an online forum, the website owner should be required to record the IP address of the individual who made the post and should be required to store this information for five years. This information may be required by law enforcement or people suing for defamation, doxing, or impersonation and must be turned over with search warrants or subpoenas.
7. No website owner should be able to hide her identity in a domain name registration. Every website owner should be required to provide an address in a domain name registration where he can be served with civil claims, subpoenas, search warrants, etc. for content on the website.
8. A website owner should be liable for defamation, doxing, or impersonation by a website user if the website owner doesn't delete the defamation, doxing, or impersonation after it's

complained about by the subject of the defamation, doxing, or impersonation. In the United States, courts have interpreted section 230 of the Communications Decency Act (CDA) to give website owners immunity from defamation by website users (Browne-Barbour, 2015; Communications Decency Act, 1996). In the United Kingdom, under the Defamation Act 2013, a website owner can be liable for defamation by a website user if it isn't deleted after being complained about (Defamation Act 2013, 2013).

9. Search engines should be stopped from indexing and displaying hyperlinks to websites notorious for defamation or doxing. There should also be public pressure on search engine companies to stop indexing and displaying hyperlinks to websites notorious for defamation or doxing.
10. Archiving websites including Google should be stopped from caching or archiving websites notorious for defamation or doxing. There should also be public pressure on archiving website companies to stop caching or archiving websites notorious for defamation or doxing. If disinformation is removed from a website, it will still appear in search engine caches until they are updated. If a webpage is changed or taken down, archiving websites shouldn't be making old information available to the public.
11. Search engines should be required to follow injunctions to remove hyperlinks to defamation, doxing, or impersonation on third party websites as well snippets of defamation, doxing, or impersonation on third party websites from search engine return pages.
12. Foreign defamation, doxing, or impersonation judgments must be enforceable in the U.S. It would be impossible for a middle class or poor person in a developing country who is being defamed, doxed, or impersonated on an American website to afford a lawyer in the U.S. to handle a civil claim. People should be able to sue for defamation, doxing, or impersonation in their own countries and get defamation, doxing, or impersonation judgments enforced in the U.S. A defamation judgment in one country should be enforceable in all other countries.

CONCLUSION

Online defamation, doxing, and impersonation are three of the major problems of the information age. Twitter needs to reform its policies as described in this research paper. Also, the laws and public policies need to be updated as described in this research paper.

Also, the public needs to be better educated on how to fight back against these problems. The author of this research paper previously made recommendations on educating the public to combat online defamation, doxing, and impersonation (Solo, 2021).

New research and development fields are needed to develop algorithms and software that can find, flag, or remove misinformation and disinformation. The author of this research paper previously proposed a field called *misinformation identification engineering* (Solo, 2021) to develop algorithms and software to find, flag, or remove misinformation and disinformation on websites and in other documents.

REFERENCES

Adikpo, J. A. (2019). Fake Online News: Rethinking News Credibility for the Changing Media Environment. In I. E. Chiluya & S. A. Samoilenko (Eds.), *Handbook of Research on Deception, Fake News, and Misinformation Online* (pp. 152-166). IGI Global. URL: <https://www.igi-global.com/chapter/fake-online-news/230752>

Assay, B. E. (2019). Social Media and the Challenges of Curtailing the Spread of Fake News in Nigeria. In I. E. Chiluya & S. A. Samoilenko (Eds.), *Handbook of Research on Deception, Fake News, and Misinformation Online* (pp. 226-263). IGI Global. URL: <https://www.igi-global.com/chapter/social-media-and-the-challenges-of-curtailling-the-spread-of-fake-news-in-nigeria/230756>

Balakrishnan, V., Khan, S., Fernandez, T., & Arabnia, H. R. (2019). Cyberbullying Detection on Twitter Using Big Five and Dark Triad Features. *Elsevier Journal of Personality and Individual Differences* (The Official Journal of the International Society for the Study of Individual Differences (ISSID)), *141*, 252-257. URL: <https://www.sciencedirect.com/science/article/pii/S0191886919300364>

Banerjee, S., & Chua, A. Y. K. (2019). Toward a Theoretical Model of Authentic and Fake User-Generated Online Reviews. In I. E. Chiluya & S. A. Samoilenko (Eds.), *Handbook of Research on Deception, Fake News, and Misinformation Online* (pp. 104-120). IGI Global. URL: <https://www.igi-global.com/chapter/toward-a-theoretical-model-of-authentic-and-fake-user-generated-online-reviews/230748>

Bradshaw, S., & Howard, P. N. (2019). *The Global Disinformation Order: 2019 Global Inventory of Organised Social Media Manipulation*. Computational Propaganda Research Project. Oxford Internet Institute, University of Oxford. URL: <https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2019/09/CyberTroop-Report19.pdf>

Browne-Barbour, V. S. (2015). Losing Their Licence to Libel: Revisiting § 230 Immunity. *Berkeley Technology Law Journal*, *30*(2), 1505-1560. URL: https://btlj.org/data/articles2015/vol30/30_2/1505-1560_Browne%20Barbour.pdf

Chiluya, I. E., & Samoilenko, S. A. (Eds.). (2019). *Handbook of Research on Deception, Fake News, and Misinformation Online*. IGI Global. URL: <https://www.igi-global.com/book/handbook-research-deception-fake-news/218293>

Collins, M. (2011). *The Law of Defamation and the Internet, Third Edition*. Oxford University Press.

Comlekci, M. F. (2020). Combating Fake News Online: Turkish Fact-Checking Services. In K. Dalkir & R. Katz (Eds.), *Navigating Fake News, Alternative Facts, and Misinformation in a Post-Truth World*

(pp. 273-289). IGI Global. URL: <https://www.igi-global.com/chapter/combating-fake-news-online/249516>

Communications Decency Act, United States, 47 U.S.C. § 230. (1996). URL: <https://uscode.house.gov/view.xhtml?req=communications+decency+act+section+230>

Cox, C. (2014). Protecting Victims of Cyberstalking, Cyberharassment, and Online Impersonation through Prosecutions and Effective Laws. *Jurimetrics*, 54(3), 277-302. URL: https://www.jstor.org/stable/24395601?seq=1#page_scan_tab_contents

Dale, T. (2019). The Fundamental Roles of Technology in the Spread of Fake News. In I. E. Chiluya & S. A. Samoilenko (Eds.), *Handbook of Research on Deception, Fake News, and Misinformation Online* (pp. 122-137). IGI Global. URL: <https://www.igi-global.com/chapter/the-fundamental-roles-of-technology-in-the-spread-of-fake-news/230750>

Dalkir, K., & Katz, R. (Eds.) (2020). *Navigating Fake News, Alternative Facts, and Misinformation in a Post-Truth World*. IGI Global. URL: <https://www.igi-global.com/book/navigating-fake-news-alternative-facts/236998>

Defamation Act 2013, United Kingdom. (2013). URL: <http://www.legislation.gov.uk/ukpga/2013/26>

Delellis, N. S., & Rubin, V. L. (2020). 'Fake News' in the Context of Information Literacy: A Canadian Case Study. In K. Dalkir & R. Katz (Eds.), *Navigating Fake News, Alternative Facts, and Misinformation in a Post-Truth World* (pp. 89-115). IGI Global. URL: <https://www.igi-global.com/chapter/fake-news-in-the-context-of-information-literacy/249504>

Grazulis, A., & Rogers, R. (2019). Ridiculous and Untrue—FAKE NEWS!": The Impact of Labeling Fake News. In I. E. Chiluya & S. A. Samoilenko (Eds.), *Handbook of Research on Deception, Fake News, and Misinformation Online* (pp. 138-151). IGI Global. URL: <https://www.igi-global.com/chapter/ridiculous-and-untrue--fake-news/230751>

Guadagno, R. E., & Guttieri, K. (2019). Fake News and Information Warfare: An Examination of the Political and Psychological Processes from the Digital Sphere to the Real World. In I. E. Chiluya & S. A. Samoilenko (Eds.), *Handbook of Research on Deception, Fake News, and Misinformation Online* (pp. 167-191). IGI Global. URL: <https://www.igi-global.com/chapter/fake-news-and-information-warfare/230753>

Hage, H., Aimeur, E., & Guedid, A. (2020). Understanding the Landscape of Online Deception. In K. Dalkir & R. Katz (Eds.), *Navigating Fake News, Alternative Facts, and Misinformation in a Post-Truth World* (pp. 290-317). IGI Global. URL: <https://www.igi-global.com/book/navigating-fake-news-alternative-facts/236998>

Holdme, A. (2022, May 6). Did Sky Ferreira turn down a date with Elon Musk? Dazed Media. URL: <https://www.dazeddigital.com/life-culture/article/56052/1/did-sky-ferreira-say-turn-down-a-date-with-elon-musk>

Kaufman, M. (2018). March 8. Twitter users are twice as likely to retweet fake news stories than authentic ones. *Mashable*. URL: <https://mashable.com/2018/03/08/twitter-users-retweet-fake-news-study/>

Koch, C. M. (2016). To Catch a Catfish: A Statutory Solution for Victims of Online Impersonation. *University of Colorado Law Review*, 88(1). URL: http://lawreview.colorado.edu/wp-content/uploads/2017/01/12.-88.1-Koch_FinalRevised.pdf

Lee, D. (2019, December 6). Elon Musk wins defamation case over 'pedo guy' tweet about cover. BBC News. URL: <https://www.bbc.com/news/world-us-canada-50695593>

Mach, L. T. (2019). The Rise of Professional Facebook Content Generators in Vietnam: A Fake News Campaign against the Betibuti Founder. In I. E. Chiluya & S. A. Samoilenko (Eds.), *Handbook of Research on Deception, Fake News, and Misinformation Online* (pp. 209-225). IGI Global. URL: <https://www.igi-global.com/chapter/the-rise-of-professional-facebook-content-generators-in-vietnam/230755>

Marsh, E. J., Cantor, A. D., & Brashier, N. M. (2016). Believing that Humans Swallow Spiders in Their Sleep: False Beliefs as Side Effects of the Processes that Support Accurate Knowledge. *Psychology of Learning and Motivation*, 64, 93-132. URL: <https://www.sciencedirect.com/science/article/pii/S0079742115000341>

Moura, M. A., & de Paula, L. T. (2020). Cognitive Authority, Accountability, and the Anatomy of Lies: Experiments to Detect Fake News in Digital Environments. In K. Dalkir & R. Katz (Eds.), *Navigating Fake News, Alternative Facts, and Misinformation in a Post-Truth World* (pp. 259-272). IGI Global. URL: <https://www.igi-global.com/chapter/cognitive-authority-accountability-and-the-anatomy-of-lies/249515>

Nielsen, G. (2020). Populism, Fake News, and the Flight from Democracy. In K. Dalkir & R. Katz (Eds.), *Navigating Fake News, Alternative Facts, and Misinformation in a Post-Truth World* (pp. 238-257). IGI Global. URL: <https://www.igi-global.com/chapter/populism-fake-news-and-the-flight-from-democracy/249513>

Ottomocar, S. L. C. (2020). Brazilian Policy and Actions to Fight Against Fake News: A Discussion Focused on Critical Literacy. In K. Dalkir & R. Katz (Eds.), *Navigating Fake News, Alternative Facts, and Misinformation in a Post-Truth World* (pp. 204-221). IGI Global. URL: <https://www.igi-global.com/chapter/brazilian-policy-and-actions-to-fight-against-fake-news/249511>

Pal, A., & Banerjee, S. (2019). Understanding Online Falsehood from the Perspective of Social Problem. In I. E. Chiluya & S. A. Samoilenko (Eds.), *Handbook of Research on Deception, Fake News,*

and *Misinformation Online* (pp. 1-17). IGI Global. URL: <https://www.igi-global.com/chapter/understanding-online-falsehood-from-the-perspective-of-social-problem/230742>

Reynard, L. J. (2019). Troll Farm: Anonymity as a Weapon for Online Character Assassination. In I. E. Chilwa (Ed.), *Handbook of Research on Deception, Fake News, and Misinformation Online* (pp. 392-419). IGI Global. URL: <https://www.igi-global.com/chapter/troll-farm/230765>

Rezayi, S., Balakrishnan, V., Arabnia, S., & Arabnia, H. R. (2018). Fake News and Cyberbullying in the Modern Era. *Proceedings of the International Conference on Computational Science and Computational Intelligence (CSCI 2018)*. IEEE CPS. URL: <https://ieeexplore.ieee.org/document/8947876>

Reznik, M. (2013). Identity Theft on Social Networking Sites: Developing Issues of Internet Impersonation. *Touro Law Review*, 29(2), article 12. URL: <https://digitalcommons.tourolaw.edu/cgi/viewcontent.cgi?article=1472&context=lawreview>

Solo, A. M. G., & Bishop, J. (2011). The New Field of Network Politics. *Proceedings of the 2011 International Conference on e-Learning, e-Business, Enterprise Information Systems, and e-Government (EEE'11)*. URL: <http://worldcomp-proceedings.com/proc/p2011/EEE5223.pdf>

Solo, A. M. G., & Bishop, J. (2014). Conceptualizing Network Politics following the Arab Spring. In A. M. G. Solo (Ed.), *Handbook of Research on Political Activism in the Information Age* (pp. 231-239). IGI Global. URL: <http://www.igi-global.com/chapter/conceptualizing-network-politics-following-the-arab-spring/110681>

Solo, A. M. G., & Bishop, J. (2016). Network Politics and the Arab Spring. *International Journal of Civic Engagement and Social Change (IJCESC)*, 3(1), 23-27. URL: <http://www.igi-global.com/article/network-politics-and-the-arab-spring/149855>

Solo, A. M. G., & Bishop, J. (2017). Conceptualizing Network Politics following the Arab Spring: An African Perspective. In J. Bishop (Ed.), *The Digital Media Reader* (pp. 205-212). Crocels Press.

Solo, A. M. G. (2011). The New Fields of Public Policy Engineering, Political Engineering, Computational Public Policy, and Computational Politics. *Proceedings of the 2011 International Conference on e-Learning, e-Business, Enterprise Information Systems, and e-Government (EEE'11)*. URL: <http://worldcomp-proceedings.com/proc/p2011/EEE5211.pdf>

Solo, A. M. G. (2014). The New Interdisciplinary Fields of Political Engineering and Computational Politics. In A. M. G. Solo (Ed.), *Political Campaigning in the Information Age* (pp. 226-232). IGI Global. URL: <https://www.igi-global.com/chapter/the-new-interdisciplinary-fields-of-political-engineering-and-computational-politics/109123>

Solo, A. M. G. (2017). An Overview of the New Interdisciplinary Fields of Political Engineering and Computational Politics for the Next Frontier in Politics. *Proceedings of the 2017 International Conference on Computational Science and Computational Intelligence (CSCI'17)*. URL: <https://ieeexplore.ieee.org/document/8561084>

Solo, A. M. G. (2019a). *Brief on Effectively Combatting Cyberbullying and Cyberlibel by Online Hate Groups for the Study on Online Hate of the Standing Committee on Justice and Human Rights for the House of Commons of Canada*. Standing Committee on Justice and Human Rights, House of Commons of Canada. URL : <https://www.ourcommons.ca/Content/Committee/421/JUST/Brief/BR10520155/br-external/SoloAMG-e.pdf>

Solo, A. M. G. (2019b). *Mémoire sur la lutte efficace contre les actes de cyberintimidation et de diffamation en ligne commis par des groupes haineux présenté au Comité permanent de la justice et des droits de la personne de la Chambre des communes du Canada dans le cadre de son étude sur la haine en ligne*. Standing Committee on Justice and Human Rights, House of Commons of Canada. URL: <https://www.noscommunes.ca/Content/Committee/421/JUST/Brief/BR10520155/br-external/SoloAMG-10061182-f.pdf>

Solo, A. M. G. (2019c). Combating Online Defamation and Doxing in the United States. *Proceedings of the 2019 International Conference on Internet Computing and Internet of Things (ICOMP'19)*. URL: <https://csce.ucmss.com/cr/books/2019/LFS/CSREA2019/ICM3560.pdf>

Solo, A. M. G. (2019d). The Interdisciplinary Fields of Political Engineering, Public Policy Engineering, Computational Politics, and Computational Public Policy. In A. M. G. Solo (Ed.), *Handbook of Research on Politics in the Computer Age*. IGI Global. URL: <https://www.igi-global.com/book/handbook-research-politics-computer-age/228093>

Solo, A. M. G. (2020). Fighting Online Defamation, Doxing, and Impersonation. *Proceedings of the International Conferences: Internet Technologies & Society and Sustainability, Technology and Education 2020*. URL: <http://www.iadisportal.org/digital-library/fighting-online-defamation-doxing-and-impersonation>

Solo, A. M. G. (2021). Educating the Public to Combat Online Defamation, Doxing, and Impersonation. In A. M. G. Solo (Ed.), *Cases on Technologies in Education from Classroom 2.0 to Society 5.0*. IGI Global. URL: <https://www.igi-global.com/chapter/educating-the-public-to-combat-online-defamation-doxing-and-impersonation/289193>

Stengel, R. (2019). *Information Wars: How We Lost the Global Battle Against Disinformation and What We Can Do About It*. Grove Press.

Sternberg, P. M. (2019). *The Guide to Internet Defamation and Website Removal*. AuthorHouse.

Vosoughi, S., Roy, D., & Aral, S. (2018). The spread of true and false news online. *Science*, 359(6380), 1146-1151. URL: <https://science.sciencemag.org/content/359/6380/1146>

Watts, C. (2018). *Messing with the Enemy: Surviving in a Social Media World of Hackers, Terrorists, Russians, and Fake News*. Harper.