

another paucity in action that brought the state-sponsored misinformation *en masse* on social media in the first place [42].

8.2 Ethical Considerations

The purpose of our study was not to generalize to a population; rather, to explore the contemporary hacktivists' relationship with misinformation in depth. To avoid misleading readers, we did not report percentages, names, or tools, tactics, and procedures mentioned during the interviews. A full moral evaluation of the suggested countering and/or utilizing misinformation is out of scope of this paper, though we condemn any action of leaks, doxing, exposure, or rumors that could result in an individual harm of any form. We are careful with our study not to infringe upon the hacktivist's aesthetics nor to cause any negative actions with our findings.

We would, however, point out that our engagement with, rather than a disavowal of, the hacktivists can help in refining and revisiting some of the over-simplistic hacktivism portraits of toxic vigilantism, nihilism, and criminality [39]. While we maintain that each operation – misinformation hacktivism related or not – has to be morally justified separately, we find reasonable to identify with the ideas and suggestions put forth by the hacktivists in our study, as they are in conformity with the Levy's hacker ethos [65] and the democratic vision of the Internet [43]. We also accept and support the idea of "fight fire with fire" action identified in our findings, as it seeks to fill a resistance void arising from a scale mismatch between institutional regulation, lax participation policies and perverse incentives of all the platforms, as well as the experience of living with misinformation in our everyday discourse [105].

8.3 Limitations

Our research was limited in its scope to U.S. hacktivists, therefore we exercise caution to the generalization of the results across the entire Internet activist community worldwide. Many hacktivist operations are often in the center of debates regarding the dimensions of civil disobedience, political participation, legality, and the ethical use of Internet technologies [105]. Our results pertain neither to append the permissiveness nor the disapproval of the these operations, rather, to voice the opinion of the hacktivists as the unique and engaged Internet minority. Even with such a relatively small sample we gathered in our study, we got a wide variety of insights to which many other hacktivists could well disagree and propose other models, approaches, and visions of dealing with misinformation.

We are aware that our results represent the contextualization informed by all forms of misinformation that currently exist on social media. Therefore, we are careful to avoid any predictive use of our results in future misinformation campaigns. Importantly, we do not know if, when, and how the hacktivists in our sample used the proposed counter-misinformation tools,

tactics, and procedures. Our results do not provide blanket justification for any frivolous use of them across social media and any other online spaces. We note that this study reported on the evolving experience of dealing with misinformation by hacktivists and might miss some important aspects of meting out the truth on social media. We advise caution to this, as we see our work as a synergistic line of scientific inquiry addresses an important gap in voicing the opinions of those that actually introduced the means for mass producing of misinformation online in the first place.

8.4 Future Work

Our future research will continue to trace the way the hacktivist community engages with misinformation. We are interested to expand our work beyond U.S. and work with hacktivists across the globe, as misinformation is contextual to the geopolitical makings in the space where many of them operate. We are set to further explore the intersection between hashtag activism and hacktivism for the same cause of countering misinformation as such synergistic activities do already emerge in some form, as the case with the #NAFO campaign on Twitter. Here, we would devote much attention to the new misinformation "battlefield" of platforms for short videos such as TikTok and Instagram. It would be useful to study the emergent circumstances in which misinformation hacktivism mobilizes and empowers ordinary users to join future "Troll [target] Day" operations and catalogue their experiences with such participation. Of equal importance, too, would be to further study the use of "misinformation-against-(mis)information" as in the case of #OpJane to learn both the benevolent and potentially malevolent aspects of this approach.

9 Conclusion

Reflecting the communitarian ideals of free information and disobedience to authority, the hacktivists in our study showed a determination for a radical response against the reprehensible act of spreading falsehoods on social media. As misinformation is consequential to the trolling and memes of the early days of hacktivism, it is appreciative to learn that the contemporary hacktivists are outwardly against such a nefarious appropriation of their aesthetics. It is encouraging to reveal that hacktivists also advocate for general misinformation literacy as a strategic asset against an undemocratic Internet. These findings, we hope, will empower ordinary users who share the same action space in reprobating misinformers for the sake of maintaining the vision of democratic Internet.

References

- [1] Shiza Ali, Mohammad Hammas Saeed, Esraa Aldreabi, Jeremy Blackburn, Emiliano De Cristofaro, Savvas

- Zannettou, and Gianluca Stringhini. Understanding the effect of deplatforming on social networks. In *13th ACM Web Science Conference 2021*, WebSci '21, page 187–195, New York, NY, USA, 2021. Association for Computing Machinery.
- [2] Jennifer Allen, Cameron Martel, and David G Rand. Birds of a feather don't fact-check each other: Partisanship and the evaluation of news in twitter's birdwatch crowdsourced fact-checking program. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*, CHI '22, New York, NY, USA, 2022. Association for Computing Machinery.
- [3] Omar Alonso, Vasileios Kandylas, Serge-Eric Tremblay, Jake M Hofman, and Siddhartha Sen. What's happening and what happened: Searching the social web. In *Proceedings of the 2017 ACM on Web Science Conference*, pages 191–200, 2017.
- [4] Janna Anderson and Lee Rainie. The future of truth and misinformation online. 2017.
- [5] Anonymous. Operation jane initiated. we're totally going to mess with texas. #anonymous, 2021.
- [6] Ahmer Arif, Leo Graiden Stewart, and Kate Starbird. Acting the part: Examining information operations within# blacklivesmatter discourse. *Proceedings of the ACM on Human-Computer Interaction*, 2(CSCW):1–27, 2018.
- [7] JP Armstrong. Twitter as a channel for frame diffusion? hashtag activism and the virality of# heterosexualpride-day. *Rise of the Far Right: Technologies of Recruitment and Mobilization*, page 87, 2021.
- [8] Corey H. Basch, Zoe Meleo-Erwin, Joseph Fera, Christie Jaime, and Charles E. Basch. A global pandemic in the time of viral memes: Covid-19 vaccine misinformation and disinformation on tiktok. *Human Vaccines & Immunotherapeutics*, 17(8):2373–2377, 2021.
- [9] Ross W. Bellaby. An ethical framework for hacking operations. *Ethical Theory and Moral Practice*, 24(1):231–255, 2021.
- [10] Yochai Benkler, Robert Faris, and Hal Roberts. *Network propaganda: Manipulation, disinformation, and radicalization in American politics*. Oxford University Press, 2018.
- [11] Davide Beraldo. Unfolding #anonymous on twitter: The networks behind the mask. *First Monday*, 27(1), 2023/01/20 2022.
- [12] Jonathan Bishop. Trolling for the lulz?: using media theory to understand transgressive humor and other internet trolling in online communities. In *Transforming politics and policy in the digital age*, pages 155–172. IGI Global, 2014.
- [13] Amanda S. Bradshaw. #doctorsspeakup: Exploration of hashtag hijacking by anti-vaccine advocates and the influence of scientific counterpublics on twitter. *Health Communication*, 0(0):1–11, 2022.
- [14] Jack Brewster, Lorenzo Arvanitis, Valerie Pavilonis, and Macrina Wang. Beware the 'new google:' tiktok's search engine pumps toxic misinformation to its young users, 2022.
- [15] David Bromell. *Deplatforming and Democratic Legitimacy*, pages 81–109. Springer International Publishing, Cham, 2022.
- [16] Victoria Carty. *Social Movements and New Technology*. Taylor and Francis, 2018.
- [17] Jin-Hee Cho, Scott Rager, John O'Donovan, Sibel Adali, and Benjamin D. Horne. Uncertainty-based false information propagation in social networks. *Trans. Soc. Comput.*, 2(2), jun 2019.
- [18] Miyoung Chong. Discovering fake news embedded in the opposing hashtag activism networks on twitter: #gunreformnow vs. #nra. *Open Information Science*, 3(1):137–153, 2019.
- [19] Matteo Cinelli, Walter Quattrociocchi, Alessandro Galeazzi, Carlo Michele Valensise, Emanuele Brugnoti, Ana Lucia Schmidt, Paola Zola, Fabiana Zollo, and Antonio Scala. The covid-19 social media infodemic. *Scientific reports*, 10(1):1–10, 2020.
- [20] E Gabriella Coleman. Logics and legacy of anonymous. *Second International Handbook of Internet Research*, pages 145–166, 2020.
- [21] Gabriella Coleman. *Hacker, hoaxer, whistleblower, spy: The many faces of Anonymous*. Verso books, 2014.
- [22] Christopher T Conner and Nicholas MacMurray. The perfect storm: A subcultural analysis of the q-anon movement. *Critical Sociology*, 48(6):1049–1071, 2022.
- [23] Ellen Cornelius. Anonymous hacktivism: Flying the flag of feminist ethics for the ukraine it army. 2022.
- [24] John Corner. Fake news, post-truth and media-political change, 2017.

- [25] Brian Creech. Fake news and the discursive construction of technology companies' social power. *Media, Culture & Society*, 42(6):952–968, 2020.
- [26] Michael Dahan. Hacking for the homeland: Patriotic hackers versus hacktivists. In *Proceedings of the 8th International Conference on Information Warfare and Security (Iciw-2013)*, pages 51–57, 2013.
- [27] Philipp Darius and Fabian Stephany. How the far-right polarises twitter: 'hashjacking' as a disinformation strategy in times of covid-19. In Rosa Maria Benito, Chantal Cherifi, Hocine Cherifi, Esteban Moro, Luis M. Rocha, and Marta Sales-Pardo, editors, *Complex Networks & Their Applications X*, pages 100–111, Cham, 2022. Springer International Publishing.
- [28] Glenn Diesen. *Conclusion: Anti-Russian Propaganda of a West in Relative Decline*, pages 255–258. Springer Nature Singapore, Singapore, 2022.
- [29] Renee DiResta, Kris Shaffer, Becky Ruppel, David Sullivan, Robert Matney, Ryan Fox, Jonathan Albright, and Ben Johnson. The tactics & tropes of the internet research agency. 2019.
- [30] Ullrich K. H. Ecker, Stephan Lewandowsky, John Cook, Philipp Schmid, Lisa K. Fazio, Nadia Brashier, Panayiota Kendeou, Emily K. Vraga, and Michelle A. Amazeen. The psychological drivers of misinformation belief and its resistance to correction. *Nature Reviews Psychology*, 1(1):13–29, 2022.
- [31] Abbas Ehsanfar and Mo Mansouri. Incentivizing the dissemination of truth versus fake news in social networks. In *2017 12th System of Systems Engineering Conference (SoSE)*, pages 1–6, 2017.
- [32] Luca Follis and Adam Fish. *3 When to Hack*, pages 73–111. 2020.
- [33] Deen Freelon, Alice Marwick, and Daniel Kreiss. False equivalencies: Online activism from left to right. *Science*, 369(6508):1197–1201, 2020.
- [34] Deen Freelon, Charlton D McIlwain, and Meredith Clark. Beyond the hashtags: # ferguson, # blacklives-matter, and the online struggle for offline justice. *Center for Media & Social Impact, American University, Forthcoming*, 2016.
- [35] Gordon Gauchat. Politicization of science in the public sphere: A study of public trust in the united states, 1974 to 2010. *American sociological review*, 77(2):167–187, 2012.
- [36] Jordana J. George and Dorothy E. Leidner. From clicktivism to hacktivism: Understanding digital activism. *Information and Organization*, 29(3):100249, 2019.
- [37] Paolo Gerbaudo. From cyber-autonomism to cyber-populism: An ideological history of digital activism. *tripleC: Communication, Capitalism & Critique*, 15(2):477–489, May 2017.
- [38] Claire Goforth. 'anonymous' hackers have a message for texas abortion 'snitch' sites: We're coming for you, 2021.
- [39] Luke Goode. Anonymous and the political ethos of hacktivism. *Popular Communication*, 13(1):74–86, 2015.
- [40] Atilla Hallsby. Psychoanalysis against wikileaks: resisting the demand for transparency. *Review of Communication*, 20(1):69–86, 2020.
- [41] Max Halupka. Clicktivism: A systematic heuristic. *Policy & Internet*, 6(2):115–132, 2014.
- [42] Jason Hannan. Trolling ourselves to death? social media and post-truth politics. *European Journal of Communication*, 33(2):214–226, 2018.
- [43] Masayuki Hatta. Cowboys and the eternal september transfiguration of hacker aesthetics. *Annals of Business Administrative Science*, page 0210923a, 2021.
- [44] Nolan Higdon, Emil Marmol, and Mickey Huff. Returning to neoliberal normalcy: Analysis of legacy news media's coverage of the biden presidency's first hundred days. In *The Future of the Presidency, Journalism, and Democracy*, pages 255–273. Routledge, 2022.
- [45] Matthew Hindman and Vlad Barash. Disinformation, 'fake news' and influence campaigns on twitter. 2018.
- [46] Philip N Howard, Bharath Ganesh, Dimitra Liotsiou, John Kelly, and Camille François. The ira, social media and political polarization in the united states, 2012–2018. 2019.
- [47] Laura Illia. Passage to cyberactivism: how dynamics of activism change. *Journal of public affairs.*, 3(4), 2003–11.
- [48] Jane Im, Eshwar Chandrasekharan, Jackson Sargent, Paige Lighthammer, Taylor Denby, Ankit Bhargava, Libby Hemphill, David Jurgens, and Eric Gilbert. Still out there: Modeling and identifying russian troll accounts on twitter. In *12th ACM Conference on Web Science, WebSci '20*, page 1–10, New York, NY, USA, 2020. Association for Computing Machinery.
- [49] Leanna Ireland. We are all (not) anonymous: Individual- and country-level correlates of support for and opposition to hacktivism. *New Media & Society*, 0(0):14614448221122252, 0.