

Fight Fire with Fire: Hacktivists' Take on Social Media Misinformation

Filipo Sharevski¹, Ben Kessell¹

¹DePaul University, Chicago, IL

SOUPS 2023



Internet and the Hacker Ethic

The Internet → Unowned and unregulated space → A new set of moral values governing the actions in this space

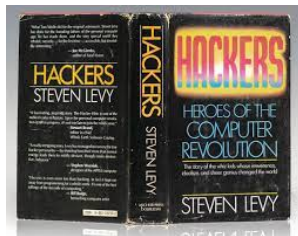
Hacker culture → Maintain a democratic vision of the Internet → resistance to the neoliberal appropriation of the cyberspace

Tenets of the hacker ethic → Sharing, Openness, Decentralization, Free access to computers, World Improvement:

Access to computers should be unlimited and total

All information should be free

Mistrust authority—promote decentralization



Internet, Hackers, and Activism

Hactivism → Anonymous, political retribution, performed in secret, operates within the cyberspace, usually with impunity

Internet → Hacking, website defacement, DDoS, doxing, leaks, account hijacking

Culture → Collectivization

“Ops” - #OpKKK, #OpFerguson, #OpISIS

Memes - Lol Cats on 4chan

Trolling - Rickrolls, #TrollISIS

Hashtag activism → Public, political mobilization, operates primarily on the streets, subject to the dangers of violence, harassment

Internet → Self-organization and participation in the sociopolitical struggle

Culture → Social mobilization

Movements - #metoo, #takeaknee, #BLM

Memed Against - Hijacking, co-opting

Trolled Against - Counter hashtagging



Hacking, Activism, and Misinformation

Appropriation → Trolling, memes, twitter bombs, falsehoods → *coutner the hacker ethic*

For the “lulz” → *weaponizing trolling* → Impolite, aggressive, disruptive, and manipulative targeting

Anti the “power” → *weaponizing memes* → Appropriate new political contexts together with viral hashtags

Exploit the “hashtag” → *weaponizing hashtag activism* → Cultural infiltration, political dissent



Jenna Abrams @Jenn_Abrams · May 6

You come into my country and you ask me to change our traditions because it offends you #refugeesnotwelcome

Retweet 165 Like 185 ...



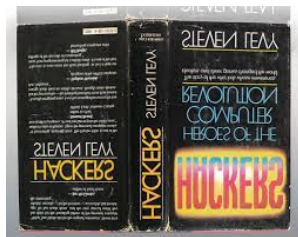
Misinformation and the Hacker Ethic

Against the public good → Misinformation rivals the supply of truth and facts and impedes the access to truth and facts in a society

Information disorder → Misinformation catalyzes polarization and emotionally-charged participation, less democratic and more neoliberal-appropriated Internet

Behind a shadow authority → State-sponsored trolling, misinformation for hire

Centralized narrative manufacturing → Obstructs independent truth discovery and dissemination



Hactivists' Response?



RQ1 → How do contemporary hacktivists conceptualize the social media misinformation ecosystem?

RQ2 → What actions do hacktivists deem appropriate in response to misinformation on social media?

RQ3 → In what directions do the hacktivists see the misinformation ecosystem evolving toward in the future?

Sampling criteria → 18+; US; active contributors in the hacktivist community

Profiles → Challenging online far-right extremism, help tracking criminals, and uncovering foreign countries' information operations

Levy's hacktivists → Active prior to 2014

Gender		
Female 8 (36.4%)	Male 13 (59.1%)	Non-Binary 1 (4.5%)



Misinformation Conceptualization

Current state → Trolling and meme dissemination has been hijacked for nefarious purposes

I remember using sock puppet accounts way back in the early 2000s running forum raids as a [REDACTED], specifically to run/post misinformation on other forums online. It was mostly for laughs, but we were massive monsters in those days. The only real major difference is these days is that the sock puppets are automated and put in action for keeping people tribalistic and resistant to opposing views.

Misinformation recipe → Self-proclamation of expertise, cultivating followers, playing on confirmation bias

For example, look at the [REDACTED]. This person said they were a founding member of Anonymous and lots of people believed them. The person has spoken at conferences about it and even got jobs because of it. Literally dig slightly into that and it's clear that no one in the Anonymous community can vouch for the person and there's no evidence of them being linked. So, people are just too lazy to check stuff out because this person is kinda selling a story that fits with what they think so it must be true



Misinformation Mental Models

Political (counter)argumentation → Plain ignorance and stubbornness to hear anything contrary to one's own political opinion

I think that people have learned that spreading disinformation through social media, Twitter for example, it's one of the best ways to get a word out. Twitter readers won't fact check things, especially if it aligns along with a political ideology people are passionate about so this word gets effectively to them. They'll believe whatever you tell them, and I think this is because there's a serious lack of, at least in the US, critical thinking education in schools.

"Truth" authority → People are entitled to see both sides of a proverbial political coin

Political tribalism → Easier to demonize people with different opinions and political attitudes and avoid scrutinizing the like-minded ones

Playbook → Sophisticated utilization of trolling and memes on such a massive scale

Turf → Overshadows and complicates an access to other more factual or useful information



Misinformation Countering

Counterstrike → Leaking, doxing, deplatforming

I've exposed threat actors after tracing their activity and positively identifying them. Unfortunately, this is somewhat of a Bushido violation amongst fellow hackers but I am not concerned with such things. Some of these clowns have it coming to them. There was one person who went by the handle ██████ who had been sexually harassing women, cyberstalking them, creating several sock puppet accounts, and just generally being a real nuisance in the community. Well, I doxed that person's real name on Twitter but I didn't post their address. Some fellow 'infosec' pros didn't appreciate that I did so but honestly, the person had it coming and I don't regret it. I was careful about what I shared so no physical harm came to the them.

Levy's Hacker Ethics → There is more ideological aspect of it to fight d/misinformation

Triage → Curtail misinformers' ability to gain followers

Disruption → Deplatforming, exposing (e.g. #OpJane)



Misinformation Evolution

Advanced tactics → Orchestrated saturation → shitposts, absurd trolling, and ridiculing memes

Latent, yet coordinated psychological warfare → Psychologists rip apart these people, conduct serious OSINT to find incriminating leaks on them, and even pay for billboards and radio ads to publicly shame them

Misinformation Literacy → Misinformation social contract; teaching hacking and misinfo tactics in school curricula

Misinformation hacktivism → Hacking against using falsehoods in furthering political causes



Implications, Limitations, Ethics, Future Work

Implications → Backfiring, interpersonal conflicts, emerging platforms (e.g. TikTok, BitChute...), alt-platforms

Ethics → We do not grant any exemption nor condone engaging in morally dubious or illegal acts (e.g. GamerGate)

Impartiality → Our results alone serve neither as an approval nor a call for any hacktivist action

Evolved Levy's Hacker Ethics → No leak, doxing, or exposure action should cause anyone else harm (physical, reputation, mental)

Limitations → Variety of hacktivist perspectives, absence of hashtag activism, US-centric study



Thank you!

Questions, Comments, Concerns



Twitter: @ACALaboratory, @B3n_5mash

https://via.library.depaul.edu/cdm_etd/47/