

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

Filipo Sharevski  
*DePaul University*

Benjamin Kessell  
*DePaul University*

## Abstract

In this study, we interviewed 22 prominent hacktivists to learn their take on the increased proliferation of misinformation on social media. We found that none of them welcomes the nefarious appropriation of trolling and memes for the purpose of political (counter)argumentation and dissemination of propaganda. True to the original *hacker* ethos, misinformation is seen as a threat to the democratic vision of the Internet, and as such, it must be confronted on the face with tried hacktivists' methods like deplatforming the "misinformers" and doxing or leaking data about their funding and recruitment. The majority of the hacktivists also recommended interventions for raising misinformation literacy in addition to targeted hacking campaigns. We discuss the implications of these findings relative to the emergent recasting of hacktivism in defense of a constructive and factual social media discourse.

## 1 Introduction

Steven Levy's portrayal of the hacker culture in his 1984 book *Hackers* largely remains the most influential reference to the public's general view of hackers [43, 65]. Recasting them Robin Hood-style activists committed to a democratic vision of the Internet [97], Levy asserts that the hacker ethos embodies several sacrosanct postulates to the public good, notably that (i) *all information should be free*, and (ii) *authority should be mistrusted and decentralization promoted* [65].

Later-day Internet hackers shifted the ideological tendency for autonomy in the cyberspace towards a vision of the Internet as a popular space for sharing any information that can nevertheless be politicized and weaponized against the neoliberal elites responsible for economic and social disarray [37]. Turning Internet activism into a form of socio-political resistance online [58], enabled a functional selection of issues that no longer necessitated a long preparation [74]. This, in turn, resulted in almost instant convergence and coordination of activities in response to the issues of interest that, over the years, became publicly visible through mass media coverage [47].

The Internet activism, expectedly, bifurcated to online campaigns concerned with the protection of the Internet as a relatively unregulated and unowned space (e.g. Anonymous, WikiLeaks, Snowden [21, 114, 116]) and online campaigns concerned with the protection of human rights and the environment (e.g. the Occupy movement, Arab Spring, Pirate Party [59, 80]). The former activism – or *hacktivism* – often is anonymous, performed in secret, and operates with a kind of impunity that the Internet technologies seem to afford so far [117]. The later activism – or *hashtag activism* – usually is public, openly used the Internet for political mobilization, operates primarily on the streets, and subjects to the dangers of crowd violence, harassment, and arbitrary arrest [100].

The hashtag activism historically utilized various Internet technologies such a petition websites (e.g. MoveOn.org for organizing political protests) or e-mail communication (e.g. Tea Party's campaign to reduce government spending and taxation) [16], but the advent of social media sites like Twitter, Facebook, and YouTube truly accelerated the self-organization and participation in the sociopolitical struggle (e.g. the #BlackLivesMatter and #SchoolStrike4Climate movements [34]). While the essential dependence on social media is apparent, both in a historical context and for the future of the hashtag activism [56], the relationship between the hacktivism and social media is a bit more complicated.

Hacktivists, in contrast, hacked various Internet technologies such as defacing websites [98], breaking into systems to "leak" and "dox" private documents [114, 118], and storm systems with traffic to cause a Denial-of-Service (DOS) [81]. Hacktivists' foray in social media mirrors these actions as campaigns were undertaken for hijacking/defacement of social media accounts (e.g., Anonymous's #OpKKK campaign [128]), doxing individuals on Twitter (e.g. the students of Covington High School [70]), and DoS Twitter topics (e.g. #IranTalks campaign [86]). But hacktivists also hacked the social media affordances for content amplification (e.g. Stay-WokeBot [36, 102]), early instances of trolling (e.g. Rick-rolls [101]), and sharing memes (e.g. Lol Cats on 4chan [21]).

Despite the intuitive versatility of social media for such

subversive operations, hacktivism became largely inactive on the mainstream platforms following some high profile run-ins with the legal authorities of the leading hacktivists [53, 124]. The apparent absence of hacktivism created a vacuum where no one actively challenged the elites, defended freedom of expression, and appended the vision of democratic social media participation. It took little time, unfortunately, for this vacuum to be appropriated by state-sponsored actors hijacking the hacking playbook for actions aimed not just against the neoliberal elites but the entire social order [32]. Bot-style amplification aided political trolling and sharing of memes in the aftermath of Brexit campaign in the UK [24] and the 2016 elections in the US [10]. The crucial difference in these instances was that the amplified memes and trolling were not pranks but damaging fake news, emotionally-charged memes, and conspiracy theories that instead of unifying the social media crowds for a cause, divided them in opposition camps pitted against each other [111].

In response to such a large-scale disruption on the social media turf, one would have plausibly expected that the hacktivists will retaliate and confront, expose, or counter hack the state-sponsored “trolls” [135]. Misinformation, back to the Levy’s depiction of hacker’s ethics [65], runs counter the (i) *all information should be free* postulate because it undermines the basic utility of information as a public good (i.e. truth and facts do not dwindle in supply as more people “consume” them and truth and facts are available to all people in a society) [31]. Misinformation also runs counter the (ii) *authority should be mistrusted and decentralization promoted* postulate because it is promulgated by a state-sponsored “shadow authority,” as evidence confirms in the aftermath of the Brexit and the 2016 US elections [48, 73, 134]. Surprisingly, the hacktivists never struck back [11], though they clearly poses the capabilities to do so, as witnessed in the Anonymous’s #OpISIS campaign, for instance, where the collective flagged about 101,000 Twitter accounts attributed to the Islamic-State [49].

The absence of response to misinformation on social media by the hacktivist community seemed quite perplexing and, in our opinion, worthy of in-depth inquiry with active “hackers” that still operate in the spirit of the Levy’s code of ethics [65]. Through personal connections and snowballing sampling, we identified 22 prominent hacker figures and set down for at least an hour-long interview with each of them to learn their take on the misinformation ecosystem, on responses to falsehoods on social media, and the way misinformation impacts and shapes the hacktivists’ agenda in the future. We found a consensus among the hacktivists against the present forms of misinformation as an ammunition for political counter(argumentation) and external propaganda. They were adamant to deplatform, dox, and expose every “misinformer” that they believe is polluting the social media discourse, and suggested ways to improve the general misinformation literacy among users in addition to these targeted operations.

To situate our study in the intersection between the hack-

tivist counter-culture and the rise of misinformation on platforms, we review the interplay between Internet activism, social media, and false information in Section 2. We look in the broader context of misinformation in Section 3 to highlight the pressing need of hacking action to reclaim the social media space true to Levy’s vision of Internet as an information exchange to the public good. In Section 4 we outline our research design and methodology. Sections 5, 6, and 7 expand on our findings and we discuss the implications of the hackers’ disposition to social media misinformation in Section 8. Finally, Section 9 concludes the paper.

## 2 Internet Activism and Social Media

### 2.1 Hashtag Activism

Online social media activism – or *slacktivism*, *clicktivism* – emerged on popular platforms as a repertoire of low-risk, low-cost expressive activities for advocacy groups’ agenda setting and political participation [99]. Social media users participated in petitions, changed personal avatars, added picture filters in support of a cause, and simply “liked” posts as an act of participation [41]. Slacktivists quickly realized they could use virality as a distinctive social media affordance to their advantage and move to use hashtags as the main drivers of mobilization, raising awareness, and demanding sociopolitical change. The practice of *hashtag activism* was instrumental for the success of social movements like #metoo, #takeaknee, and #BlackLivesMatter, allowing for mainstream visibility, expression of solidarity, and statement of victimhood [115]. This success, in turn, inspired a plethora of other movements advocating for health, human rights, social justice, and environmental issues to spur across all social media platforms and remain active within the public discourse [52].

The materialization of the hashtag activism, however noble, had to deal with the obvious threat of *hashtag hijacking* or the encroachment on viral hashtags to inject contrary perspectives into a discourse stream [126]. This “hack” against the internet activism is not just adding noise or attempting to result in a DoS, but also to disseminate hateful narratives and dilute the campaign itself (e.g. the hijacking of the #metoo hashtag [69]). Another similar threat is the *hashtag co-opting* or the contentious co-opting of the rhetoric of popular social movements (e.g. #HeterosexualPrideDay campaign co-opting the language of the mainstream LGBT movement [7]). Equally threatening is the *counter hashtagging* that concocts similar hashtags to garner opposition to well-established movements (e.g. #BlueLivesMatter countermovement to police reform in reaction to #BlackLivesMatter [61]). These antagonistic appropriations of the social media virality, consequently, enabled political extremism to creep in the public discourse and embroil users in an emotionally-charged participation [95].

In a state of emerging social media polarization, it was a question of time when fake news, offensive memes, and

conspiracy theories would be weaponized against the hashtag activism (e.g. the proliferation of fake news in the #Gunreformnow vs #NRA Twitter battle [18]). What was initially expected to remain on the fringes of the mainstream hashtag activism [33], quickly turned into an information disorder on a mass scale. Now the hashtag hijacking and co-opting developed *in parallel* with the main theme of activism, and for that, a steady and substantive feed of false and unverified information was needed. The emotionally-charged participation loomed into a global health panic (e.g. #FlattenTheCurve hashtag hijacking for spreading COVID-19 misinformation [27]) and moral panic (e.g. the QAnon's co-opting of #SaveTheChildren hashtag [83]) in addition to the already growing political panic [85].

## 2.2 Hacktivism

*Hacktivism* was a term that “Omega,” a member of the Texas-based computer-hacking group *Cult of the Dead Cow* (cDc) coined in 1996 in an email to the cDc listserv [75]. Characterized with the increasingly political ethos of hacking-for-cause, hacktivists primarily leveraged technology to advance human rights and protect the free flow of information in campaigns against the UK, US, and Chinese governments, as well as the UN [88]. In as much as hackers individually roamed the Internet, socialization was at the proper time as many of them needed establishing a strong hacktivist network. Hacktivists’ penchant for humorous memes (LOLCats) and gag hyperlinks (Rickrolls) [91] attracted an army of hackers to Christopher Poole’s 4chan.org social media website, bringing to life the notorious collective Anonymous [75].

While hacktivists never displayed a predictable trajectory of their cyberoperations and political program [21], they narrowly utilized social media for self-promotion – announcing operations with an #Op prefixed hashtags [11] – and furthering a complex relationship with other Internet activists. Anonymous cried foul on Twitter when WikiLeaks puts millions of its documents behind a pay wall [40], but also launched Operation #Ferguson of doxing the St. Louis County police chief daughter’s information in response to the shooting of the black teenager Michael Brown [9]. Hacktivists, in solidarity to the Arab spring uprisings, sent a care package composed of security tools and tactical advice though downplayed the touted “Twitter Revolution” [21].

True to their credo for utilizing Internet technologies against oppression, including social media, hacktivists launched the #OpKKK to “unhood approximately 1000 Ku Klux Klan members” hacked by gaining access to a KKK Twitter account in support of #BlackLivesMatter protesters in Ferguson, Missouri [128]. After a several years hiatus, perhaps due to arrests of some of the leading Anonymous hacktivists, the group resurfaced during the 2020 #BlackLivesMatter protests in response to the killing of George Floyd [54]. This time, in addition to the leaking of a trove of 269 giga-

bytes of confidential police data (dubbed *BlueLeaks* [64]), the hacktivists launched social bot operations to amplify a support towards #BLM and criticize police actions.

Hacktivists also utilized Internet technologies in the context of cyberwarfare. For example, the #OpIsis operation, in which lists of tens of thousands of Twitter accounts that purportedly belonged to members of ISIS or its sympathizers were leaked, was launched in response to the terrorist attacks in France in 2015 [77]. Here, in addition to the leaks, hacktivists also waged a meme war and called for a “Troll ISIS Day” to provoke and disrupt ISIS-supported social media [76]. The Anonymous group in early 2022 took on Twitter to declare a “cyber war” to Russia in response to the Ukrainian invasion, launching DoS attacks against Russian’s Federal Security Service’s website and hacking Russian streaming services to broadcast war videos from Ukraine [104].

## 3 Internet Activism and Misinformation

### 3.1 Grassroots Misinformation Operations

Hacktivists, perhaps inadvertently, authored or gave popularity to the most utilized primitives for creating, propagating, amplifying, and disseminating misinformation - *trolling* and *memes*. This negative externality is unfortunate as trolling and memes were initially used by Anonymous against what they perceived a “misinformation campaign” by the Church of Scientology [75]. The “anon” members on 4chan.org practically *hijacked* the term “troll” – initially meaning provoking others for mutual enjoyment – to abusing others for members’ own enjoyment by posting upsetting or shocking content (usually on the \b channel of 4chan.org [21]), harassing users (e.g. mocking funeral websites [12]), and spreading rumors [62]. What Anonymous did for the “lulz” (a brand of enjoyment etymologically derived from laughing-out-loud (lol)), nonetheless, showed the ease with which one could exploit the Internet technologies to be impolite, aggressive, disruptive, and manipulative to users’ emotional states [21].

Trolling initially came in textual format as comments to posts, bulletin boards, and websites “deindividualized” people’s lived experience for the “lulz” [12]. Gradually, hacktivists popularized a multimedia format of trolling or “memes,” where textual commentary is superimposed over well-known imagery, typically representing different forms of power, such as political leaders, the police, and celebrities [76]. Memes, perhaps, were the actual rite of passage to true hacktivism – moving away from the early LOLCats – as they seek to deconstruct the power represented, contest censorship, and provide political commentary [87]. Memes as content were put to hacktivist use *en masse* in operations like “Troll ISIS day,” where Anonymous proliferated memes with rubber-duck heads or rainbow stripes to ridicule ISIS propaganda imagery and disinformation narratives on Twitter [76]. Spread together with satirizing hashtags (e.g. #Daeshbags), the trolling memes

achieved a cultural virality that brought hacktivists' into the mainstream discourse online [92]. What the hacktivists did with the memes nonetheless, showed the ease with which one could disrupt, challenge, reimagine, and appropriate new political contexts by harnessing the virality and visibility of content spread on social media [84].

### 3.2 Mainstream Misinformation Operations

The hacktivists' playbook of trolling and meme dissent, though initially targeted *against* misinformation, was skillfully appropriated *for* crafting and disseminating misinformation from 2014 onward, coinciding with the period of hacktivist inactivity [11]. The playbook alone, at first, was insufficient to the objectives of widespread political disruption as it necessitated a support network of individuals and/or accounts on social media for any alternative narratives to gain traction. But the "appropriators" – privy of prior campaigns of disinformation and with the support of nation-state governments [113] – need not to look further as "sock puppet" accounts were already utilized for spreading political falsehoods (e.g., Martha Coackey's "twitter bomb" disinformation campaign [85]). Having all the ingredients for exploiting the virality of social media and users' familiarity with emotionally-charged discourse, the "appropriators" established *troll farms* in the wake of the UK's Brexit campaign and 2016 US elections [73, 135].

The "army" behind the troll farms were particularly clever to append their social bots with "sock puppet" accounts that imitate ordinary users to systematically micro-target different audiences, foster antagonism, and undermine trust in information intermediaries [6]. Playing both sides in the emotionally-charged discourse already unravelling on social media, the troll farms posed as authentic, cultural competent personas (e.g. so-called "Jenna Abrams" account [130]), as well as vocal supporters of hashtag activism (counter) movements (e.g. BlackToLive in #BlackLivesMatter and SouthLoneStar in #BlueLivesMatter [119]). They also appropriated the hashtag hijacking (e.g., #elections2016 and #ImVotingBecause tagging of quotes about Donald Trump and against Hillary Clinton [3]), hashtag co-opting (e.g. #BlackGunsMatter and #syrianlivesmatter [29]), and counter hash tagging (e.g. #NoDAPL against the Dakota Access Pipeline [45]). The troll farms even had the audacity to impersonate the Anonymous themselves (e.g. the @\_anonymous\_news impersonation of the "Your Anonymous News" twitter account [20]).

The "meme game" of the troll farms was equally sophisticated and appended the initial success of their operations [82]. Testing the waters with war-related memes regarding the opposition/support of the conflict in Syria [29], the troll farms capitalized on both the meme trolling and the Internet activism by spreading political memes through their Blacktivist social media accounts and co-opting Wikileaks in exploiting the leak of sensitive documents from the Democratic National Committee (DNC) [71]. Memes were also used to amplify

conspiracy theories (e.g. QAnon, Pizzagate, and the murder of Seth Rich [132]), Texas secessionism (e.g. if Brexit why not #Texit [50]), and direct attacks (e.g. crooked Hillary [46]).

While the initial campaigns of the troll farms have been tracked, exposed, and brought into attention [29, 46], the social media discourse never really recovered from the watershed appropriation of the Internet activism for the purpose of conducting information operations [111]. Worse, the troll farm brand of political dissent was adopted by populist accounts that were keen on disseminating misinformation beyond just politics [51]. The trolling pandemonium spilled out of control with the COVID-19 pandemic as rumors, conspiracy theories, fake news, and out-of-context spins plagued the social media by hijacking the dominant hashtags like #COVID19, #coronavirus or #DoctorsSpeakUp [13], co-opting hashtags like #plandemic [60] and counter hash tagging with hashtags like #COVIDIOT [110]. Memes were distributed in conjunction with deepfake videos on platforms like YouTube [96] and TikTok [8] as well as blatant fake news on alt-platforms like Gab [19] to effectively reach a self-perpetuating bedlam of misinformation Internet counter-activism.

## 4 Hacktivism and Misinformation

In a radical state of ravaging misinformation campaigns on social media with no end in sight, one could wonder what the original activists on the Internet have to say in response. The unravelling of falsehoods clearly is a serious threat to the democratic vision of the Internet [97], as misinformation facilitated the rise of non-democratic communities contesting even factual knowledge and science (e.g. anti-vaxers, climate change deniers, etc. [127]). Hacktivists, as we have seen in Section 2, have fiercely opposed early misinformation campaigns in the past, but their means to do so were the "hijacked" for the mass produced misinformation of later. One could attribute the paucity of hacktivists' involvement in the passing of the techno liberal order of the Internet as the rise of partisan-divided trust in facts and the politicization of science were already underway [35], but that alone is not a sufficient showstopper for action.

Regardless of any new Internet order, there is a reasonable expectation that one should still act upon the Levy's sacrosanct postulates [65], even if that is within an ecosystem polluted with misinformation. In addition to the public good arguments, misinformation is in conflict with the *all information should be free* postulate as it creates "information disorder" that, by the token of catalyzing polarization and emotionally-charged participation online, gives even more power to the neoliberal elites for perpetuating the economic and social (media) disarray [25]. Misinformation also conflicts with the *authority should be mistrusted, and decentralization promoted* postulates as it stands in the way of independent truth discovery and dissemination online [67]. Should the new brand of reprehensible misinformation, therefore, be

on the top of the hacktivists' agenda already?

## 4.1 Research Questions

To explore the gap in hacktivism in regards mass misinformation, we invited prominent members of the hacktivist community to answer the following research questions:

- **RQ1:** How contemporary hacktivists conceptualize the social media misinformation ecosystem?
- **RQ2:** What action hacktivists deem appropriate in responding to misinformation on social media?
- **RQ3:** In what directions do the hacktivists see the misinformation ecosystem evolve in the future?

## 4.2 Sample

Our study was approved by the Institutional Review Board (IRB) of our institution before we invited, through personal contacts, and snowballing sampling the hacktivists for a virtual interview session with open-ended questions, listed in the [Appendix](#). We sampled a population who were 18 years or older, from the United States, that is an active contributor in the hacktivist community, and has a history of such an involvement that we could reasonably verify. We used zoom interviews where we offered the possibility for the participants to choose if they want to use a video feed or not. Every interview was recorded, stored in a secure server, and manually transcribed and communicated with the interviewee to obtain an approval before we started the qualitative analysis.

Overall, we ended with a sample of total of 22 participants, all of which agreed to participate voluntarily. The demographics are given in Table 1. We made a deliberate attempt to produce a sample that is not a male-only or male-dominated, as previous studies indicate that the hacktivist community is imbalanced in regards gender [121]. The participation in the study was not anonymous to us as researchers, but we deliberately avoid using definitive numbers and potentially identifiable information in reporting of our results to preserve their anonymity to the general population, as a condition for their participation. In some cases, we used a direct censoring of names in citing participants' responses. We allowed the participants to skip any question they were uncomfortable answering. The interviews took around an hour to complete.

Table 1: Sample Demographic Distribution

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

## 4.3 Methods and Instrumentation

To ensure validity to the task of conceptualizing misinformation, we decided to introduce the participants in the main study to the generalized definition of misinformation on social media proposed by Wu et al. [129]. Another reason was to avoid confusion between past trolling and memes "for the lulz" and present alternative narratives that involve information operations, rumors, conspiracy theories, fake news, hoaxes, and clickbait. The hacktivists in our sample were invited to speak about their profiles, activity, and agendas online, before we asked their take on misinformation on social media. The qualitative responses were coded and categorized in respect: a) antecedents to misinformation; b) mental models of misinformation; c) countering misinformation through leaking, doxing, and deplatforming; d) anti-misinformation "ops" (operations); e) counter-misinformation tactics; f) misinformation literacy; and g) misinformation hacktivism.

Two independent researchers analyzed the approved interview transcriptions, achieving a strong level of inter-coder agreement (Cohen's  $\kappa = .82$ ). We utilized a thematic analysis methodology to identify the themes and sub-themes most saliently emerging from the responses in our sample. The themes were summarized to describe the conceptualization, response, and evolution of misinformation in the view of the contemporary hacktivists we sampled. In reporting the results, we utilized as much as possible verbatim quotation of participants' answers, emphasized in "*italics*" and with a reference to the participant as either **PX** or **[PX]**, where **P** denotes **participant** and **X** denotes the **number** of the participant in the sample (ordered by the time of participation).

## 4.4 Hacktivists' Profiles

The hacktivists in our sample, true to the original ethos, represent the voice for advocacy and contemporary policy discussion. While they did not disclose their current operations, several of them hinted they are involved in tracking the rise of the far-right extremism, cybercriminals, as well as the information warfare part of the Ukraine invasion. A couple of the hacktivists' agenda was leaking documents from companies and nation-state agencies as manifestation of their information freedom advocacy. Few of the hacktivists explicitly mentioned they still create and disseminate memes and participate in the "old school" trolling. And several of the hacktivists did actual *hacking* as in analyzing security problems (e.g. ransomware) and providing free tools for helping ordinary Internet users fend off related threats.

The majority of the hacktivists noted they have been active for a long time, being brought into the world of computers in childhood or early adolescence. Some of them resorted to hacktivism as a way to protect themselves against online bullies and some of them in response to nation-states offensive operations online, notably ones linked to China and Russia.

Several of them started with hacking operating systems to enable unrestricted access to games and/or bypass parental controls. While most of the participants in our sample cited curiosity as their driver to enter the “hacktivist conglomerate” and keep on hacking, there were some participants citing a deliberate determination for cybersecurity education activism.

## 5 Misinformation Conceptualization

Social media users conceptualize misinformation, evidence shows, in more than one model that narrowly focuses on inherently fallacious information [109]. Beyond just fake news, misinformation is equally conceptualized as form of *political (counter)argumentation* where facts do selectively appear in alternative narratives relative to political and ideological contexts, often taken *out-of-context* with speculative intentions. Misinformation is also seen as *external propaganda* that includes *manufactured* facts and factoids disseminated and amplified online with division-creating intentions. Given the radical transformation of the trolling and memes over time, our first research question aimed to learn the hacktivists’ take on this transformation in the context of the competing conceptualizations amongst ordinary social media users.

### 5.1 Antecedents to Misinformation

The participants in our sample agree that trolling and meme dissemination has been hijacked for nefarious purposes, lamenting that what was a “*deliberate action mostly for laughs, now is an automated operation for keeping people tribalistic and resistant to opposing views*” [P13]. The use of “*sock puppets for running forum raids in the old days of hacktivism*” [P4], unfortunately, was not enough a serious threat for social media to implement “*strict policies of who and how can participate in the public discourses early on*” [P1] and counter to their business model of “*monetizing every possible engagement on their platforms*” [P14].

Mainstream social media companies were accused of directly enabling the “*information disorder*” as their models of engagement pushed “*less educational content the more an issue was important and demanded action*” [P14]. This disorder played in the hands of the neoliberal elites, media outlets, and news organizations run by “*billionaires detached from reality to gain further control over public spaces*” as P1 put it. In the view of our participants, misinformation “*has always been there*” and pointed to the combination of “*self-proclamation of expertise online, cultivating followers, and playing on confirmation bias*” as the recipe the very hacktivists showed it works well in seeding misinformation:

“*For example, look at the [redacted]. He said he was a founding member of Anonymous and lots of people believed him. He 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 guy and there’s no evidence of him being linked. So, people are just too lazy to check stuff out because this guy is kinda selling a story that fits with what they think so it must be true*” [P3].

### 5.2 Mental Models of Misinformation

The predominant mental model of misinformation amongst the hacktivists in our sample was the *political (counter)argumentation* where the information disseminated on social media for the sake of furthering a political argument or agenda [109]. In the original version of trolling and meme sharing the misinformation was seen as an alternative expression of disagreement, revolt, or ridicule without any context, but the contemporary trolling and memes is brought in the political context as a ready-made content for expression of political attitudes [90]. Despite that fact checking is widely available (and even suggested to users when content is moderated on social media [108]), the political appropriation of misinformation thrives because “*people won’t fact check things and perpetuate them as long as these things align with their political ideology*” [P2]. The reason why most social media users “*fall for misinformation*” is *plain ignorance and stubbornness to hear anything contrary to their own political opinions*” [P3] which results from “*a serious lack of, at least in the U.S., critical thinking education in schools*” [P2].

In the view of the majority hacktivists in our study, “*both sides of the political spectrum spread misinformation and it further enables political polarization*” [P13]. While they acknowledge that “*the misinformation on social media is often identified with right-wing opinions*” [P6], hacktivists recognize that “*we overuse the terms misinformation and disinformation to describe anything that is not a leftist opinion or fact*” [P7]. They point to the misinformation “stickiness” where the repeated exposure to speculative and false statements make them appear truthful [66], becoming the main theme of every social media discourse. For example, P3 refers to the Biden’s laptop saga [44], which in their view “*has been politically disinfoed [sic] to death to the point that the laptop leaks are irrelevant and can’t be trusted as an evidence*.”

Misinformation as political counter(argumentation) bothers the hacktivists as it conflicts with the *all information should be free* postulate, which in turn forces mainstream social media platforms to “*restrict the flow of information*” [P10]. Misinformation, in the view of P10, should not be restricted because “*people are entitled to see both sides of a proverbial political coin so the platforms must allow them to do so, otherwise by only showing heads or tails people will speculate about what’s on the other side and assume the worst*.” The restriction of information on platforms conflicts with the *mistrust of authority and promote decentralization* hacker postulate because “*self-appointed elites to define what constitutes*

‘truth’” [P14]. It also forces “*people to become rather tribalistic and a priori suspicious of people with different views*” [P]. The “political tribalism” on social media [2], in turn, makes it “*easier to demonize people with different opinions and political attitudes and avoid scrutinizing the like-minded ones*” [P2], which plays directly in the hands of the “misinformers.”

As for the “misinformers”, our participants unequivocally identified the state-sponsored “appropriators” that hijacked the original hacktivist playbook to spread *external propaganda* on social media. That nation-states enjoyed a reputation for promulgating disinformation in the past was not a news to the hacktivists (e.g. “*Russia has always been really good at it*” [P2]), but instead what caught them aback was the “*audacity and the sophistication*” [P4] in utilizing trolling and memes on such a massive scale [134]. Reflecting on this shift in online operations, P3 believes that “*disinfo ops [sic] and hacking our intellectual property is all these nation-states are left with because they can’t beat us militarily or economically.*” Not necessarily neoliberal, but nonetheless authoritarian, the elites behind the external propaganda in equal degree conflicts with the *mistrust of authority and promote decentralization* hacker postulate because is a “*blatant effort to control the social media turf and the mass of population spending their time there*” [P15]. The external propaganda nature of disinformation also conflicts with the *all information should be free* hacker postulate in the view of the hackers in our sample because “*overshadows and complicated an access to other more factual or useful information*” [P2].

## 6 Active Countering of Misinformation

Literature on misinformation focuses on helping the social media *users* discern falsehoods with strategies for “*pre-bunking*” i.e. forewarning and preemptive refutation of the falsehoods [68] or “*debunking*” i.e. providing users verifiable corrections of the falsehoods from credible sources to break the illusion of truth [30, 93]. An *algorithmic* is also available for the mainstream social media platforms (the alternative ones do not deem misinformation as a problem [107]) that leverages natural language processing, image analysis, or metadata to detect trolling and memes [50, 51, 122]. Platforms also have the option for algorithmic “*soft*” moderation by either obscuring trolling and memes with warnings covers or attaching warning labels [108, 125] and “*hard*” moderation for removing or suspending misinformer accounts [63]. None of these solutions, however fends of troll farms and meme disseminators effectively, so we wanted to know what hacktivists have to propose instead in the second research question.

### 6.1 Leaking, Doxing, and Deplatforming

Suspending user accounts by social media platforms for breach of their code of conduct is referred to as “*deplatforming*” [1]. In the context of hacktivism, it takes a border mean-

ing as hacktivists do investigative work that entails leaking and doxing but also confrontation with the misinformers that, in their subjective view, breaches the vision of democratic Internet. For example, hacktivists did a massive API scrapping of the alt-platform Parler to leak data that tied users to the Capitol Riots and the QAnon conspiracy [94], which in turn resulted in a massive account deplatforming on Twitter [15]. These activities spur operations to confront and expose the QAnon conspirators on social media (e.g. @QAnonAnonymous [22]), amongst which some of our hacktivists have a direct role in “*dismantling the Qanon infrastructure*” [P2].

The deplatforming targets political misinformation campaigns where our hacktivists “*compiled and leaked dossiers on individuals spreading hateful propaganda and those who seek to sow the seeds of violence*” [P1] on social media. These operations were targeted both on “*individual spreaders, nation-states, even companies with murky records*” [P2]. Several mentioned their direct operations for exposing disinformation relative to the “*Ukrainian conflict*” [P5], praising the work of the Ukrainian IT Army outfit for dispelling the myth that Ukraine is committing genocide against Russians in the Donbas region [23]. Hacktivists were dedicated in “*doxing companies and governmental agencies in response to the political meddling in the US internal affairs from places like Russia, Iran, and China*” [P8]. Misinformation “*sanctioned by the governments*” was targeted by hackers in attempts to deplatform prominent “*disinformation front agents on social media, like Irina Tsukerman, for example*” [P3].

Leaks and doxing were equally utilized for misinformation beyond political counter(argumentation) and external propaganda. One of the hacktivists has dedicated considerable time on exposing cryptocurrency scammers on social media and elsewhere, deeming the feeling of it as “*better than sex*” [P5]. Another was focused leaking personal details about predators on social media that spread misinformation to cover their sexual harassment and cyberstalking towards women, “*exposing both their sock puppet accounts and their real name on Twitter*” [P3]. Another pushed back against criminal misinformation by doxing “*bullies, liars, and fraudsters*” [P20] and one “*anti-cancel culture in case of minors*” hacktivist noted that they “*successfully deplatformed major participants in hate campaigns and stalking of minors*” on social media [P5].

### 6.2 Anti-Misinformation “Ops”

The hacktivists in our sample engaged in misinformation saturation ops, true to the their commitment to “*fight misinformation with more information*.” One of the hacktivists stated that it is “*expected from the hacktivist community to combat misinformation in such a way*” and noted that “*it is the sole reason they maintain a Twitter account*” [P3]. Another one seconded this posture noting that “*it is frustrating to see misinformation from others and other creators but that is the main reason I continue to post on TikTok*” [P17]. In the words

of **P2**, “*there is more ideological aspect of it when I am fighting disinformation,*” directly invoking the mission of the true hacktivists to become reflexively “*loud and determined*” to speak true information in response to the “*general assholery of misinformation on internet*” [P9].

Partaking in operation #NAFO (North Atlantic Fellas Organization) dedicated to countering Russian propaganda and disinformation in Ukraine by weaponizing memes [103], our participants materialized a combination of saturation and doxing to “*curtail misinformers’ ability to gain followers*” [P1]. They extended their work to counter “*extremists and fascists and their toxic conspiracy theories*” [P1] by disrupting their funding and deplatforming prominent followers, true to the spirit of the “Antifa” hacktivist counterculture [131]. In a similar vein, one of the hacktivists proclaimed that they “*greatly contributed in the #OpJane operation*” [P10]. #OpJane is the latest operation launched by Anonymous against Texas for enacting the anti-abortion Bill 8 that allows “*abortion bounty*” for anyone who will investigate and report abortion in the state of Texas [38]. Interestingly, in the announcement of the operation, Anonymous calls for “*fighting misinformation with enough plausible and difficult to disprove misinformation*” to make any data these bounty hunters gather as useless [5].

## 7 Misinformation Evolution

As there is virtually no cost of disseminating misinformation [85], it is unlikely that the online discourse will shed off the alternative narratives soon. If this gloomy prediction will eventually materialize [78] or the Internet will improve because the new technologies will upgrade public’s ability to judge the quality and veracity of content [4], remains an open issue. Because the hacktivists are nonetheless stakeholders in resolving this issue, our third research question aimed to bring their prediction of how online spaces will fare with trolling, memes, and falsehoods in the near future.

### 7.1 Counter-Misinformation Tactics

The hacktivists in our sample unanimously posit that “*it is hard for social media platforms to keep up with removing it, so people stepping in to help is going to be of critical importance*” [P13] for preserving a healthy discourse. The mobilization for “*justice and truth as a cause*” [P15] is important not just for curbing misinformation but “*reclaiming information back from the political hold*” [P1]. To help “*expose misinformation charlatans*” [P4], hacktivists call for maintaining a code of conduct where “*no leak, doxing, or exposure action should cause anyone else harm (physical, reputation, mental)*” [P3].

To begin with, **P3** recommends that we should “*stop treating disinformation as a freedom of speech.*” As misinformers usually use this cloak to act very aggressively on social media, the next step is to “*identify what their weakness are and what triggers them - deplatforming or provocation?*” [P14]. If

the misinformers are unresponsive spreaders, then “*exposing, doxing, and putting their real faces through OSINT*” [P15] is in due place not just on mainstream social media but also alt-platforms, forums and everywhere on Internet. If they itch for a provocation, then “*orchestrated saturation*” [P5] might work better with “*shitposts, absurd trolling, and ridiculing memes*” [P18]. Here, the hacktivists note, it is vitally important to *a priori* distance from a “*political whataboutery*” [P14] and avoid “*coming across as censorship, disagreement, canceling that only could cause argument or dismissal*” [P5].

Some of the hacktivists were on the opinion that “*doxing is not hacking anymore per se because you can get stuff with a credit card and documents could be easily faked nowadays*” [P1]. One possible tactic, proposed by **P1**, was to “*find exploits, vulnerabilities in their platforms and step-by-step expose misinformers’ amateurish way of doing trolling, using bots, and feeding think tanks to get a credibility behind their propaganda.*” Another tactic, proposed by **P2**, was “*doxing for the purpose of having advertisers pull from supporting known misinformer influencers, like for example in the case of Andy Ngo.*” Proposing more of a hybrid hacktivist tactics, **P4** suggested “*a latent, yet coordinated psychological warfare where 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.*” Along these lines, **P11** even suggested throwing the book at them, targeting them with a social engineering attack and attempting to compromise a piece of their core infrastructure, be that their servers, Internet access, or bot credentials.”

### 7.2 Misinformation Literacy

Hacktivists in our sample echo the sentiment regarding the social media users’ susceptibility to false information found in scientific literature: laziness to check facts [P2] [89], resistance to authoritative suggestions [P7] [57], allegiance [P13] [120], and simple ignorance [P16] [17]. As people that resort to action, hacktivists do feel the obligation to propose ways for addressing this susceptibility. In the view of **P5**, “*misinformation needs to be seen as something everyone is being watched for, and not just one group of people on the left or the right,*” A “*misinformation social contract*” [136] necessitates interventions such as “*a critical thinking curricula in schools*” [P18], “*teaching hacking OpSec skills as social responsibility and rise to action*” [P5], and “*forcing professional communication norms on platforms*” [P16].

As hacktivists have little control over these interventions, they were happy to help with a development of “*truth-spreading bots for a ‘standoff’ with misinformation-spreading bots*” as something that could append the practice of leaks, doxing, and exposure [P13]. They recognized that these “*truth-spreading bots*” must help ordinary users to better find and locate facts, as information literacy is the single most effective one in dispelling falsehoods [55]. Hacktivists reiter-

ate that platforms do have to let “*misinformation to float on social media and make bots visible, so they gets overwhelmed with factual information*” to demonstrate to ordinary users how to do help themselves [P14].

Regardless if these stances are realistic or not, the hacktivists in our sample believe that the current approach to raising misinformation literacy is ineffective because it does not signal an “*unbiased attitude*” [P7] to the social media users in the wrong. Instead of an educational and respectable tone, “*rather a ‘cancel culture’ infused or a ‘your opinion is wrong’ tone*” [P3] plagues any attempt to help people to navigate and locate factual information. Rejection of misinformation, as a result of misinformation literacy, must come as an agreement that “*scientific facts do not have political properties, even if the social media platforms inherently do*” [P5].

### 7.3 Misinformation hacktivism

The participants in our sample acknowledge that orchestrated *misinformation hacktivism*, bar individual instances of ops against misinformers, is largely absent from social media. For the hacktivists to assume misinformation as a worthy cause for action, the conflict between the past “hacking for political causes” and [58] future “hacking against using falsehoods in furthering political causes” [22] must be resolved. Though this conflict is complex and evolving, several of the hacktivists worried that it could nevertheless create a “*division between the hacktivists on political lines*” [P2].

As a relative threat to the misinformation activism, one participant mentioned the hijacking of the hacktivists image for self-promotion, e.g. “*some like to portrait themselves as woke gods of the web with zero fuck-ups*” [P12]. Another threat is the temptation of using misinformation against misinformation, as in the #OpJane campaign [P10]. While this strategy is true to the “fight-fire-with-fire” approach, it might backfire in circumstances where abiding to the hacktivist ethic comes secondary to expressing social and political angst on social media [79]. On top of this, one could argue that this conflict *per se* might be hard to resolve in the misinformation instance as external propaganda, because even if the hacktivists are “hacking for the homeland,” they nonetheless are doing it on political terms [26].

## 8 Discussion

### 8.1 Implications

The new brand of misinformation, our findings show, draws the ire of the hacktivists, reprehending the hijacked discourse for political and propagandistic proposes. The “fight-fire-with-fire” response – leaks, doxing, and deplatforming – though individually employed by some of the participants in our sample, is yet to be orchestrated and tested against serious disinformation outfits that, unfortunately, are still out there

on social media [48]. The early evidence outside of the US shows that this orchestration works as the IT Army leaked data from Russian organizations in response to the troll farms’ disinformation narrative that Ukraine is committing genocide against Russians in the Donbas region [23].

The hacktivists’ resoluteness to go after the misinformers would certainly have implications for the content/user moderation on social media, user participation, and future of Internet activism overall. Moderating users and content on social media was, and still is, the response by the mainstream platforms to the political and public health misinformation [108]. Alternative platforms like Gab, Gettr, and Parler, seen as the seeding grounds for this misinformation [133], on the other hand, never did, nor currently do, employ any content/user moderation [107]. While the content/user moderation incites a migration from the mainstream to the alt-platforms [133], it remains to be seen whether the deplatforming will have the same effect. Mainstream social media had a mixed response to leaks and doxing in the past (e.g. allowing WikiLeaks [114] and barring the Hunter Biden’s laptop leaks [28]), so this also adds uncertainty if and how the hacktivists’ “fight-fire-with-fire” approach will be allowed, moderated, or perhaps even forced to migrate entirely outside of the social media space.

Trolling and memes might still maintain the popularity amongst the misinformers, however, the latest modes of social media participation like short videos on TikTok open new “fronts” for both the misinformers and the hacktivists. TikTok has increasingly been tested as the next “battlefield” of alternative narratives with evidence of health and abortion misinformation [8, 112] and an individual engagement by at least one of participants. Recalling that the hacktivists’ #OpJane was waged in response to the abortion ban laws in Texas and called for “misinformation-against-(mis)information” [38], it is yet to see how the leaks, doxing, and deplatforming will materialize with meme-ified videos and trolling. TikTok claims it does health and abortion misinformation moderation [123], but evidence shows that this is lax and largely ineffective [14], adding an additional incentive for shifting the disinformation campaigns on this platform.

TikTok is also the next platform for Internet activism where the hashtag activism is appended with videos expanding the developing news narratives, such as the coverage of the Black Lives Matter movement and the Capitol riot [72]. TikTok presents content not just from viral hashtags but also their variations (e.g. #abortion but also #abortion [112]) so the threat of hashtag hijacking, co-opting, and counter hash tagging will inevitably materialize here too. This particular affordance likely will allow for weaponizing deepfakes in appending the hashtag war in near future, as they already appeared in misinformation videos about the COVID-19 pandemic on TikTok [106]. All of these developments would certainly necessitate a dynamic adaptation in the way doxing, leaking, and deplatforming is performed in order not just to avoid disintegration of the Internet activism and hacktivism, but prevent

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 Pavlonis, 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, Champaigne, 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 Brugnoli, 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, hoaxter, 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,# blacklivesmatter, 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 Lighammer, 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.

- [50] Peter Jachim, Filipo Sharevski, and Emma Pieroni. Trollhunter2020: Real-time detection of trolling narratives on twitter during the 2020 us elections. In *Proceedings of the 2021 ACM workshop on security and privacy analytics*, pages 55–65, 2021.
- [51] Peter Jachim, Filipo Sharevski, and Paige Treebridge. Trollhunter [evader]: Automated detection [evasion] of twitter trolls during the covid-19 pandemic. In *New Security Paradigms Workshop 2020*, NSPW ’20, page 59–75, New York, NY, USA, 2021. Association for Computing Machinery.
- [52] S.J. Jackson, M. Bailey, B.F. Welles, and G. Lauren. *#HashtagActivism: Networks of Race and Gender Justice*. MIT Press, 2020.
- [53] Keenan Jones, Jason R. C. Nurse, and Shujun Li. Behind the mask: A computational study of anonymous’ presence on twitter. *Proceedings of the International AAAI Conference on Web and Social Media*, 14(1):327–338, May 2020.
- [54] Keenan Jones, Jason R.C. Nurse, and Shujun Li. Out of the shadows: Analyzing anonymous’ twitter resurgence during the 2020 black lives matter protests. *Proceedings of the International AAAI Conference on Web and Social Media*, 16(1):417–428, May 2022.
- [55] S Mo Jones-Jang, Tara Mortensen, and Jingjing Liu. Does media literacy help identification of fake news? information literacy helps, but other literacies don’t. *American behavioral scientist*, 65(2):371–388, 2021.
- [56] Andreas Jungherr, Gonzalo Rivero, and Daniel Gayo-Avello. *Retrofitting Politics: How Digital Media Are Shaping Democracy*. Cambridge University Press, 2020.
- [57] Ben Kaiser, Jerry Wei, Eli Lucherini, Kevin Lee, J Nathan Matias, and Jonathan R Mayer. Adapting security warnings to counter online disinformation. In *USENIX Security Symposium*, pages 1163–1180, 2021.
- [58] Vasileios Karagiannopoulos. *A Short History of Hacktivism: Its Past and Present and What Can We Learn from It*, pages 63–86. Springer International Publishing, Cham, 2021.
- [59] Athina Karatzogianni. *Firebrand waves of digital activism 1994-2014: The rise and spread of hacktivism and cyberconflict*. Springer, 2015.
- [60] Matthew D Kearney, Shawn C Chiang, and Philip M Massey. The twitter origins and evolution of the covid-19 “plandemic” conspiracy theory. *Harvard Kennedy School Misinformation Review*, 1(3), 2020.
- [61] Vance D. Keyes and Latocia Keyes. Dynamics of an american countermovement: Blue lives matter. *Sociology Compass*, 16(9):e13024, 2022.
- [62] Allison Klempka and Arielle Stimson. Anonymous communication on the internet and trolling. *Concordia Journal of Communication Research*, 1(1):2, 2014.
- [63] Deepak Kumar, Patrick Gage Kelley, Sunny Consolvo, Joshua Mason, Elie Bursztein, Zakir Durumeric, Kurt Thomas, and Michael Bailey. Designing toxic content classification for a diversity of perspectives. In *SOUPS@ USENIX Security Symposium*, pages 299–318, 2021.
- [64] Micah Lee. *Hack of 251 Law Enforcement Webiste Exposes Personal Data of 700,000 Cops*. 2020.
- [65] Steven Levy. *Hackers: Heroes of the Computer Revolution - 25th Anniversary Edition*. O’Reilly Media, Inc., 1st edition, 2010.
- [66] Stephan Lewandowsky, John Cook, Ullrich Ecker, Dolores Albarracin, Michelle Amazeen, Panayiota Kendou, Doug Lombardi, E Newman, Gordon Pennycook, Ethan Porter, et al. *The Debunking Handbook 2020*. 2020.
- [67] Stephan Lewandowsky, Ullrich K.H. Ecker, and John Cook. Beyond misinformation: Understanding and coping with the “post-truth” era. *Journal of Applied Research in Memory and Cognition*, 6(4):353–369, 2017.
- [68] Stephan Lewandowsky and Sander van der Linden. Countering misinformation and fake news through inoculation and prebunking. *European Review of Social Psychology*, 32(2):348–384, 2021.
- [69] Simon Lindgren. Movement mobilization in the age of hashtag activism: Examining the challenge of noise, hate, and disengagement in the #metoo campaign. *Policy & Internet*, 11(4):418–438, 2019.
- [70] Alexander J Lindvall. Political hacktivism: doxing & the first amendment. *Creighton L. Rev.*, 53:1, 2019.
- [71] Darren L. Linville and Patrick L. Warren. Troll factories: Manufacturing specialized disinformation on twitter. *Political Communication*, 37(4):447–467, 2020.
- [72] Ioana Literat, Lillian Boxman-Shabtai, and Neta Kligler-Vilenchik. Protesting the protest paradigm: Tiktok as a space for media criticism. *The International Journal of Press/Politics*, 0(0):19401612221117481, 0.
- [73] Clare Llewellyn, Laura Cram, Adrian Favero, and Robin L. Hill. Russian troll hunting in a brexit twitter archive. In *Proceedings of the 18th ACM/IEEE on*

- Joint Conference on Digital Libraries, JCDL '18*, page 361–362, New York, NY, USA, 2018. Association for Computing Machinery.
- [74] Martha McCaughey and Michael D Ayers. *Cyberactivism: Online activism in theory and practice*. Psychology Press, 2003.
  - [75] Ty McCormick. Anthropology of an idea hacktivism. *Foreign Policy*, (200):24–25, May/Jun 2013.
  - [76] Ally McCrow-Young and Mette Mortensen. Countering spectacles of fear: Anonymous' meme ‘war’ against isis. *European Journal of Cultural Studies*, 24(4):832–849, 2021.
  - [77] Virginia McGovern and Francis Fortin. The anonymous collective: Operations and gender differences. *Women & Criminal Justice*, 30(2):91–105, 2020.
  - [78] Lee McIntyre. *Post-truth*. MIT Press, 2018.
  - [79] Paul Mihailidis and Samantha Viotti. Spreadable spectacle in digital culture: Civic expression, fake news, and the role of media literacies in “post-fact” society. *American behavioral scientist*, 61(4):441–454, 2017.
  - [80] Stefania Milan. *Social movements and their technologies: Wiring social change*. Springer, 2013.
  - [81] Stefania Milan. Hacktivism as a radical media practice. In *The Routledge companion to alternative and community media*, pages 550–560. Routledge, 2015.
  - [82] Ryan M Milner. *The world made meme: Public conversations and participatory media*. MIT Press, 2018.
  - [83] Rachel E. Moran and Stephen Prochaska. Misinformation or activism?: analyzing networked moral panic through an exploration of #savethechildren. *Information, Communication & Society*, 0(0):1–21, 2022.
  - [84] Mette Mortensen and Christina Neumayer. The playful politics of memes. *Information, Communication & Society*, 24(16):2367–2377, 2021.
  - [85] Eni Mustafaraj and Panagiotis Takis Metaxas. The fake news spreading plague: Was it preventable? In *Proceedings of the 2017 ACM on Web Science Conference*, WebSci ’17, page 235–239, New York, NY, USA, 2017. Association for Computing Machinery.
  - [86] Mahdi M. Najafabadi and Robert J. Domanski. Hacktivism and distributed hashtag spoiling on twitter: Tales of the #irantalks. *First Monday*, 23(4), Apr. 2018.
  - [87] Asaf Nissenbaum and Limor Shifman. Internet memes as contested cultural capital: The case of 4chan’s/b/board. *New media & society*, 19(4):483–501, 2017.
  - [88] Taylor Owen. *Disruptive power: The crisis of the state in the digital age*. Oxford Studies in Digital Politics, 2015.
  - [89] Gordon Pennycook and David G. Rand. Lazy, not biased: Susceptibility to partisan fake news is better explained by lack of reasoning than by motivated reasoning. *Cognition*, 188:39–50, 2019. The Cognitive Science of Political Thought.
  - [90] Gordon Pennycook and David G. Rand. The psychology of fake news. *Trends in Cognitive Sciences*, 25(5):388–402, 2021.
  - [91] W. Phillips and R.M. Milner. *The Ambivalent Internet: Mischief, Oddity, and Antagonism Online*. Polity Press, 2017.
  - [92] Whitney Phillips. The house that fox built: Anonymous, spectacle, and cycles of amplification. *Television & New Media*, 14(6):494–509, 2013.
  - [93] Man pui Sally Chan, Christopher R. Jones, Kathleen Hall Jamieson, and Dolores Albarracín. Debunking: A meta-analysis of the psychological efficacy of messages countering misinformation. *Psychological Science*, 28(11):1531–1546, 2017.
  - [94] David Redding, Jian Ang, and Suman Bhunia. A case study of massive api scrapping: Parler data breach after the capitol riot. In *2022 7th International Conference on Smart and Sustainable Technologies (SpliTech)*, pages 1–7, 2022.
  - [95] Eugenia Ha Rim Rho and Melissa Mazmanian. Political hashtags & the lost art of democratic discourse. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, CHI ’20, page 1–13, New York, NY, USA, 2020. Association for Computing Machinery.
  - [96] Daniel R’ochert, Gautam Kishore Shahi, German Neubaum, Björn Ross, and Stefan Stieglitz. The networked context of covid-19 misinformation: Informational homogeneity on youtube at the beginning of the pandemic. *Online Social Networks and Media*, 26:100164, 2021.
  - [97] Mark Rolfe. *Hacker: Creating the Narrative of the Digital Robin Hood*, pages 135–164. Springer Singapore, 2016.
  - [98] Marco Romagna. *Hacktivism: Conceptualization, Techniques, and Historical View*, pages 743–769. Springer International Publishing, Cham, 2020.
  - [99] Dana Rotman, Sarah Vieweg, Sarita Yardi, Ed Chi, Jenny Preece, Ben Schneiderman, Peter Pirolli, and Tom

- Glaisyer. From slacktivism to activism: Participatory culture in the age of social media. In *CHI '11 Extended Abstracts on Human Factors in Computing Systems*, CHI EA '11, page 819–822, New York, NY, USA, 2011. Association for Computing Machinery.
- [100] Rodrigo Sandoval-Almazan and J. Ramon Gil-Garcia. Towards cyberactivism 2.0? understanding the use of social media and other information technologies for political activism and social movements. *Government Information Quarterly*, 31(3):365–378, 2014.
- [101] Madelyn R Sanfilippo, Shengnan Yang, and Pnina Fichman. Managing online trolling: From deviant to social and political trolls. In *50th Annual Hawaii International Conference on System Sciences, HICSS 2017*, pages 1802–1811. IEEE Computer Society, 2017.
- [102] Saiph Savage, Andres Monroy-Hernandez, and Tobias Höllerer. Botivist: Calling volunteers to action using online bots. In *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing*, CSCW '16, page 813–822, New York, NY, USA, 2016. Association for Computing Machinery.
- [103] Mark Scott. The shit-posting, twitter-trolling, dog-deploying social media army taking on putin one meme at a time, 2022.
- [104] Dimitrios Serpanos and Theodoros Komninos. The cyberwarfare in ukraine. *Computer*, 55(7):88–91, 2022.
- [105] Philip Serracino-Inglott. Is it ok to be an anonymous? *Ethics & Global Politics*, 6(4):22527, 2013.
- [106] Lanyu Shang, Ziyi Kou, Yang Zhang, and Dong Wang. A multimodal misinformation detector for covid-19 short videos on tiktok. In *2021 IEEE International Conference on Big Data (Big Data)*, pages 899–908, 2021.
- [107] Filipo Sharevski, Amy Devine, Peter Jachim, and Emma Pieroni. “Gettr-ing” User Insights from the Social Network Gettr, 2022. [https://truthandtruthtonline.com/wp-content/uploads/2022/10/TTO\\_2022\\_proceedings.pdf](https://truthandtruthtonline.com/wp-content/uploads/2022/10/TTO_2022_proceedings.pdf).
- [108] Filipo Sharevski, Amy Devine, Peter Jachim, and Emma Pieroni. Meaningful context, a red flag, or both? preferences for enhanced misinformation warnings among us twitter users. In *Proceedings of the 2022 European Symposium on Usable Security*, EuroUSEC '22, page 189–201, New York, NY, USA, 2022. Association for Computing Machinery. <https://doi.org/10.1145/3549015.3555671>.
- [109] Filipo Sharevski, Amy Devine, Emma Pieroni, and Peter Jachim. Folk models of misinformation on social media. In *Network and distributed system security symposium*, 2023.
- [110] Filipo Sharevski, Alice Huff, Peter Jachim, and Emma Pieroni. (mis)perceptions and engagement on twitter: Covid-19 vaccine rumors on efficacy and mass immunization effort. *International Journal of Information Management Data Insights*, 2(1):100059, 2022.
- [111] Filipo Sharevski, Peter Jachim, Emma Pieroni, and Nate Jachim. Voxpop: An experimental social media platform for calibrated (mis)information discourse. In *New Security Paradigms Workshop*, NSPW '21, page 88–107, New York, NY, USA, 2021. Association for Computing Machinery.
- [112] Filipo Sharevski, Jennifer Vander Loop, Peter Jachim, Amy Devine, and Emma Pieroni. Abortion misinformation on tiktok: Rampant content, lax moderation, and vivid user experiences. *arXiv preprint arXiv:2301.05128*, 2023.
- [113] Filipo Sharevski, Paige Treebridge, Peter Jachim, Audrey Li, Adam Babin, and Jessica Westbrook. Socially engineering a polarizing discourse on facebook through malware-induced misperception. *International Journal of Human–Computer Interaction*, 38(17):1621–1637, 2022.
- [114] Micah L Sifry. *WikiLeaks and the Age of Transparency*. OR Books, 2011.
- [115] Ellen Simpson. Integrated & alone: The use of hashtags in twitter social activism. In *Companion of the 2018 ACM Conference on Computer Supported Cooperative Work and Social Computing*, CSCW '18, page 237–240, New York, NY, USA, 2018. Association for Computing Machinery.
- [116] Edward Snowden. *Permanent record*. Pan Macmillan, 2019.
- [117] Tom Sorell. Human Rights and Hacktivism: The Cases of WikiLeaks and Anonymous. *Journal of Human Rights Practice*, 7(3):391–410, 09 2015.
- [118] Kevin F Steinmetz. Hacking and hacktivism. *Shades of Deviance: A Primer on Crime, Deviance and Social Harm*, 19, 2022.
- [119] Leo G Stewart, Ahmer Arif, and Kate Starbird. Examining trolls and polarization with a retweet network. In *Proc. ACM WSDM, workshop on misinformation and misbehavior mining on the web*, volume 70, 2018.

- [120] Briony Swire-Thompson, Ullrich KH Ecker, Stephan Lewandowsky, and Adam J Berinsky. They might be a liar but they're my liar: Source evaluation and the prevalence of misinformation. *Political psychology*, 41(1):21–34, 2020.
- [121] Leonie Maria Tanczer. Hacktivism and the male-only stereotype. *New Media & Society*, 18(8):1599–1615, 2016.
- [122] William Theisen, Joel Brogan, Pamela Bilo Thomas, Daniel Moreira, Pascal Phoa, Tim Weninger, and Walter Scheirer. Automatic discovery of political meme genres with diverse appearances. *Proceedings of the International AAAI Conference on Web and Social Media*, 15(1):714–726, May 2021.
- [123] TikTok. Tiktok safety, 2022.
- [124] Justus Uitermark. Complex contention: analyzing power dynamics within anonymous. *Social Movement Studies*, 16(4):403–417, 2017.
- [125] Anthony Vance, David Eargle, Jeffrey L. Jenkins, C. Brock Kirwan, and Bonnie Brinton Anderson. The Fog of Warnings: How Non-essential Notifications Blur with Security Warnings. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*, Santa Clara, CA, August 2019. USENIX Association.
- [126] Courtland VanDam and Pang-Ning Tan. Detecting hashtag hijacking from twitter. In *Proceedings of the 8th ACM Conference on Web Science*, WebSci '16, page 370–371, New York, NY, USA, 2016. Association for Computing Machinery.
- [127] Silvio Waisbord. Truth is what happens to news. *Journalism Studies*, 19(13):1866–1878, 2018.
- [128] Jared M Wright, Kaitlin Kelly-Thompson, S Laurel Weldon, Dan Goldwasser, Rachel L Einwohner, Valeria Sinclair-Chapman, and Fernando Tormos-Aponte. Drive-by solidarity: Conceptualizing the temporal relationship between# blacklivesmatter and anonymous's# opk. *Contention*, 10(2):25–55, 2022.
- [129] Liang Wu, Fred Morstatter, Kathleen M. Carley, and Huan Liu. Misinformation in social media: Definition, manipulation, and detection. *SIGKDD Explor. Newslett.*, 21(2):80–90, nov 2019.
- [130] Yiping Xia, Josephine Lukito, Yini Zhang, Chris Wells, Sang Jung Kim, and Chau Tong. Disinformation, performed: self-presentation of a russian ira account on twitter. *Information, Communication & Society*, 22(11):1646–1664, 2019.
- [131] Weiai Wayne Xu. Mapping connective actions in the global alt-right and antifa counterpublics. *International Journal of Communication*, 14:22, 2020.
- [132] Savvas Zannettou, Barry Bradlyn, Emiliano De Cristofaro, Haewoon Kwak, Michael Sirivianos, Gianluca Stringini, and Jeremy Blackburn. What is gab: A bastion of free speech or an alt-right echo chamber. In *Companion Proceedings of the Web Conference 2018*, pages 1007–1014, 2018.
- [133] Savvas Zannettou, Tristan Caulfield, Jeremy Blackburn, Emiliano De Cristofaro, Michael Sirivianos, Gianluca Stringhini, and Guillermo Suarez-Tangil. On the origins of memes by means of fringe web communities. In *Proceedings of the Internet Measurement Conference 2018*, IMC '18, page 188–202, New York, NY, USA, 2018. Association for Computing Machinery.
- [134] Savvas Zannettou, Tristan Caulfield, Barry Bradlyn, Emiliano De Cristofaro, Gianluca Stringhini, and Jeremy Blackburn. Characterizing the use of images in state-sponsored information warfare operations by russia trolls on twitter. *Proceedings of the International AAAI Conference on Web and Social Media*, 14(1):774–785, May 2020.
- [135] Savvas Zannettou, Tristan Caulfield, William Setzer, Michael Sirivianos, Gianluca Stringhini, and Jeremy Blackburn. Who let the trolls out? towards understanding state-sponsored trolls. In *Proceedings of the 10th ACM Conference on Web Science*, WebSci '19, pages 353–362, New York, NY, USA, 2019. Association for Computing Machinery.
- [136] Melissa Zimdars and Kembrew McLeod. *Fake news: understanding media and misinformation in the digital age*. MIT Press, 2020.

## Appendix

1. How do you describe your niche, role, activity, or agenda you have online?
2. What brought you to hacking, OSINT, cyber-threat intelligence, and any operations you have taken so far?
3. Have you faced any obstacles, challenges, repercussions because of your activity?
4. Has the obstacles, challenges, repercussions affected your commitment, motivation, and vision of your actions and in what way?
5. What is your take on the increased misinformation proliferation online?
6. Have you ever engaged or considered engaging in utilizing your actions in exposing disinformation campaigns? What was the disinformation about, in what capacity you participated, and what were the outcomes you were attempting to achieve?
7. What do you think the tools, tactics, and procedures undertaken in a hypothetical *misinformation hacktivism* operation might entail?
8. What in your opinion, is the way to continue evolving this work and in what shape and form?
9. Is there anything else that you would like to add or say that is relevant to the questions we have asked so far?
10. If you would like to share some demographic information, please do - we don't require it but it will help us better contextualize your effort and story.