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 hactivist 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 mimes 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 mime 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-appoints the elites to define what constitutes*