Hacktivist or Anti-hero?

Elizabeth Simpkins

CYSE200T: Cybersecurity, Technology, and Society [19782]

Professor: Matthew Umphlet

November 30, 2024

Introduction

Protestors, before the surge of the internet, had to grab people's attention on the streets. Nowadays, most people spend most of their day on the internet than they do outside or in public functions. This is where hacktivists, digital protestors, have gone. When I first heard the word hacktivist, the first thing that came to mind was the hacktivist group that showed up around 2003 on 4chan, "an image-based internet forum" (Britannica, 2024). I have read many articles about the group and in several news-based articles, the word Hacktivist was used interchangeably with another word; cyberterrorist. While, hacktivism can cause a lot of damage, as far as financial or reputation loss, it does not include a goal of physically hurting people, compared to cyberterrorism where a lot of people can end up injured or killed. Hacktivist are people who commit digital crimes for the greater good; therefore, I believe that they are very different from cyberterrorists, and their skills can be used in the security field to expose and pinpoint flaws in a network, product, or governmental structure.

An example of what a hacktivist group does: Anonymous

One very widely known hacktivist group was Anonymous. Their actions were small at first, with harassment and small hacks towards people they did not like, but were not politically

based. They developed a new target after they were portrayed by the news media as a terrorist group (Britannica, 2024) and after the Church of Scientology incident in 2008 (Bensel, 2017). After a video of Tom Cruise praising the Church of Scientology was removed after the demands of the church for removal, Anonymous was angry with the injustice and believed it to be free speech. Anonymous "responded with DDoS attacks, prank phone calls, and black faxes sent" (Bensel, 2017). These two incidents became the reasons for Anonymous to start targeting corruption and unjust institutions. Their targets became "credit card companies, white supremacist organizations, child pornography sites, copyright protection agencies, and [governments]" (Britannica, 2024). Their actions were based on the good of the nation, but like all hacktivist groups, the ethics in their actions have been widely debated.

Hacktivists are protestors using civil disobedience as their peaceful weapon

Nonetheless, I know the thought of a group of hackers breaking into a network and rendering it completely useless sounds really bad, but if it is thought about as a type of civil disobedience, the peaceful protest of a law, it makes sense for a technology-based society. As stated, from an article on ProQuest, Hacktivism is:

> "The promotion of a sociopolitical agenda usually linked (but not limited) to ideologies typical of traditional activism and applied in cyberspace through individual and collective actions, using illegal or legally ambiguous computer hacking techniques that exploit, hinder, and disrupt the ICT infrastructure's technical features, without the use of physical violence and without gaining direct economic benefits." (Farmer, 2022, as cited in Romagna, 2019).

Looking back at civil rights movements, I remember reading about different groups, like ones led by Martin Luther King Jr., that would hold sit-ins in public establishments in order to protest against discrimination and segregation. These protestors would prevent the workers of the establishment from completing their work by occupying seats, therefore causing lack of income and the drawing of attention. I believe that this is no different than hacktivism today, since hacktivists are "nonviolent political protestors" that make their point through the use of hacking tools.

The difference between a hacktivist and a cyberterrorist

Despite media renditions of hacktivists' similarities to cyberterrorists, they really only have one similar goal in mind; the drive of a belief, however it is the execution of that belief that I believe draws a hard line between a hacktivist and a cyberterrorist. Hacktivist generally target the government and their actions, not the general public or groups affiliated with certain beliefs, which is where cyberterrorists, on the other hand, target (Farmer, 2022). Hacktivism includes a wide variety of tactics to prevent government or any other target groups from being able to function online or prevent the release of secret data. These tactics include "account hijacking, DDoS [attacks], defacement, SQL 151 injection and leaking sensitive information" (Farmer, 2022). Cyberterrorism, on the other hand, is the use of anger towards specific groups based on beliefs or backgrounds in order to create physical harm and destruction in critical infrastructures. While hacktivism is meant to create change and expose corruption, cyberterrorism's "primary objective is inflicting physical, economic or digital harm, to undermine society's support points, by instilling fear in a large portion of the population" (Ribalta, 2018). I believe that this is a serious problem because instead of finding ways to work with hacktivists, people have labeled them and called them enemies instead.

Difficulties in the criminal justice system and implementing cyber policies for the future

That being said, I am not saying that hacktivist should not be prosecuted, because "in order to be determined within civil disobedience, hacktivists have to be proven to be taking a non-violent approach, be public in demonstration, and be non-resistant to arrest or punishment" (Wulf, 2022). Hacktivism is also hard to hold accountable due to its controversial connection to the first amendment. Hacktivists' actions can be hard to determine if they are violent or not, due to the fact that people are not harmed in their attacks. Many whistleblower hacktivists, which will typically act with another hacktivist site called WikiLeaks, will leak secret government information hidden from the citizens. In one case, Bradley Manning released over 91,000 documents on WikiLeaks over government corruption. He revealed 144 civilian causalities in the Afghanistan War logs. Manning was convicted on extreme charges, but later released by the current president. These types of cases from hacktivists create questions from the other side of the argument of whether or not the allowance of this type of free speech should be allowed in every case. It is also questioned on whether or not it will hurt the U.S. (Bensel, 2017). I think that while the exposure of information is illegal, it is also the right of the people to know things as well as their right to have the "freedom of speech, press, and thought" (Bensel, 2017).

While hacktivist actions can sometimes be illegal, they still share a loyalty to the law, at least the parts that are just and fair for all, according to the founding documents (Wulf, 2022). I believe the best way to reduce the number of hacktivist-based attacks is to work with Hacktivists on problems that are widely protested against, and secure against ones that are unjust, unethical, or dangerous to the public. People can hire hacktivists to try to break into the network and find vulnerabilities, just like an ethical hacker would do. I believe that maybe there is such a strong voice coming from hacktivists because there are serious problems in government corporations,

law, and decision making in general that these people want to make the public aware of. Hacktivists are interest groups voicing their opinion, just through a different medium.

Conclusion

Overall, hacktivists resemble digital protestors, finding corruption in the government and other sites. They act through civil disobedience by rendering sites useless or presenting their arguments through government website defacement or screen messages. Hacktivists present cases of corruption and unjust matters to the public, and this can be used in security as well to uncover these types of things that unethical hackers may be exploiting or distributing. On the other side of the argument, however, Civil disobedience is seen as a way to try to justify illegal actions from interest groups that don't agree with the general public (Wulf, 2022). This is a major concern, since hacktivist groups can lean their concerns to the left or to the right as far as politics go. The ethics behind a hacktivist is hard to determine, because of the control that they can have over the government in many cases, and the actions they take to get there. I believe that hacktivists can be used for the greater good, however, in uncovering corruption and malicious activity in the unethical hacking world. There should be a limit on what the extent of hacktivist's exposure and abilities should entail, but again, this can be hard to determine how much they should be limited based on controversial views and the first amendment. As far as long-term goals for hacktivists in this field, they could be used in sending messages to customers of vulnerable products, especially when a company refuses to fix this vulnerability in their product. In the end, hacktivism is controversial from many sides, but it needs to be looked at from a different point of view. This would help people see the benefits that it could provide to the security field and to the general public for its ability to make people more included and knowledgeable about what goes on behind the scenes of our government and institutions.

References

Bensel, A. (2017). Hacktivists: Heroes, cybercriminals, or cyberterrorists? Hacktivism and the first amendment. ProQuest. https://www.proquest.com/docview/2009333012?pq-origsite=gscholar&fromopenview=true&sourcetype=Dissertations%20&%20Theses

Farmer, F. (2022). Cybercrime vs hacktivism: Do we need a differentiated regulatory approach? ProQuest. https://www.proquest.com/docview/2699050282?pq-origsite=gscholar&fromopenview=true&sourcetype=Dissertations%20&%20Theses

Ribalta, C.N. (2018). Organic bodies versus digital bodies: The differences between hacktivism and cyberterrorism https://d1wqtxts1xzle7.cloudfront.net/56564132/Thesis-Negri-libre.pdf?1526316975=&response-content-disposition=inline%3B+filename%3DOrganic_bodies_versus_digital_bodies_the.pdf&Expires=1732756766&Signature=TW9P~me2gouByXAgjuCFpnG4fUw0apvurjSwYlLeMyTSD40cZmT5kxq9O462AVluoVJAeT1P5iPTTddYCTPe9zQo~Zz2P3-ZfLyeuHGKpzerbOU02AdErm6F2YyvNBinr8-fSbHJvjzGfd6etKvQ5Ts3g91gcR1DhuEAwYxFjCwZ1b6l78gan~Q1hhnMW1QjeUlPwI-SwhXKC0TczLZcNctbxZVRhstwHuh4UFqO2Yvq0U61Tw5kYbrqhCChkGA906osbfwPVhcjfx~sSxSBhJneop0Qmq--qUw3NtDZothtlOVqlsJxL32k2nWUuBO6~ukTiP~0WDl3j-xXz9LkyQ__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA

The Editors of Encyclopaedia Britannica. (2024). Anonymous: Digital activists. Britannica. https://www.britannica.com/topic/Anonymous-hacking-group

Wulf, L. (2022). Anonymity, fidelity to law, and digital civil disobedience. SageJournals. 49(4), 358-517. https://journals.sagepub.com/doi/full/10.1177/01914537211072886