# Survey on Hacktivism

Levi Seibert
Athens State University
Athens, AL, USA
lseiber1@my.athens.edu

## ABSTRACT

Hacktivism is the use of computer technologies to perform some form of activism. Hacktivism can appear in many forms, but it has a directed focus. This paper will evaluate several published research papers and essays that help dissect this topic of hacktivism and some of the controversies that go along with it. The largest debate has to do with the confusion of hacktivism and cyberterrorism and several of the papers under consideration discuss this distinction. On a related note, several of the authors believe that cyberterrorism has not yet made an appearance in the world, and perhaps never will. The paper concludes by summarizing the discussion on hacktivism and adding some thoughts to the discussion that may prompt further discussion or research.

## KEYWORDS

Hacktivism, hacking, activism, cyberterrorism, terrorism, new media, web defacement

## 1 INTRODUCTION

In today's technological world, hacking is viewed in a very poor light. When you think of a hacker, you think of some guy in his basement frantically typing out code in order to penetrate some type of cyber defense. Once he just gets past this next firewall, he will have access to a complete network and can began to wreck his havoc. His purposes are to infiltrate a system to win fame or riches, and his motivation is to remain undetected.

While this is the stereotype that hackers have, no thanks to Hollywood, this is not always an accurate picture. Sure, there are plenty of cybercriminals and script kiddies out there, but there is also a large number of hackers who are not trying to do harm. In fact, they believe that the hacking they are doing is for the common good. They are a league of technological gurus who are passionate about some topic, whether it be religious, political, or societal, and they choose to use their hacking powers to spread their message and perhaps make a difference in the world.

These are the hacking activists, or hacktivists as they are often called. Despite what the media, or the government, might think, they are not terrorists and should not be confused with cyberwarriors. They have a mission of changing the world, but doing so peacefully. However, does this mission give them the right to break the law in order to further their activism campaigns? If not, are there better solutions available?

The following section of the paper evaluates five research papers regarding the concepts of hacktivism and cyberterrorism. The content of each paper is discussed, intermingled with some evaluations regarding the validity and impact of each. Following the five evaluations, a brief conclusion summarizes some of the common thoughts throughout the papers and presents some alternative ideas regarding the idea of hacktivism.

## 2 SURVEYS

Several authors have written articles and papers on the topic of hacktivism, with some varying looks at the subject. Some of the research is a bit dated, and therefore some of the statements/predictions made do not hold true in modern times, but based on the information and trends of the time the papers were written, they seem to point in the right direction.

### 2.1 Terrorism or Civil Disobedience

One of the most foundational papers in regards to the discussion on hacktivism is "Terrorism or Civil Disobedience: Toward a Hacktivist Ethic" by Mark Manion and Abby Goodrum from Drexel University in Pennsylvania. While the main goal of the paper is to discuss how hacktivism is often mislabeled by the media, it does provide a succinct definition and discussion of hacktivism and the use of hacking in civil disobedience.

The authors define hacktivism as the "use of computer hacking to help advance political causes", and they add the parenthetical qualification that this hacking is often clandestine. Hacktivism has been a tool used in modern world events such as the Zapatista rebellion and the occupation of East Timor. Hacktivism has been used to weigh in on subjects such as dataveillance and the commercialization of the Internet.

The authors suggest that hacktivism aims to fight two main battles: the commodification of the Internet by corporations and the violation of human rights by governments. As a result, hacktivism threatens both private industry (that is, intellectual property) and national government/security.

A related concept to hacktivism is that of electronic civil disobedience. Civil disobedience is the deliberate, yet peaceful, breaking of laws that are considered unjust. Two of the most popular examples of this are the sit-ins and protests of the Civil Rights Movement in the 1960s and the Boston Tea Party of 1773. The key part of civil disobedience is the word “civil.” Civil disobedience “does not condone violent or destructive acts” but instead uses “nonviolent means to expose wrongs, raise awareness, and prohibit the implementation of perceived unethical laws.”

Civil disobedience falls into two camps. Direct civil disobedience refers to the breaking of laws, while symbolic civil disobedience consists of indirectly drawing attention to an issue. Sit-is are examples of symbolic acts of civil disobedience, as long as the sit-ins do not break the law that the demonstrators are protesting against.

With the inception of the World Wide Web, civil disobedience has taken a turn. Instead of physical acts of disobedience, the realm of Electronic Civil Disobedience (or ECD) allows protestors to voice their opinions and spread their messages, without having to even leave their homes. ECD acts could be simple as sending emails or as complex as breaking into computer systems.

The authors do point out that there is a distinction between activists who support ECD and those that perform acts of ECD. The former, the supporting role, often engages in discussions regarding activism topics, but does not engage in any illegal activity (this is often referred to as electronic activism). The latter, however, actually performs “malicious” activity to make a statement (this is true ECD). The “maliciousness” of these actions will not cause harm; however, but they often cause a disruption of services that may lead to adverse effects on a system.

According to Manion and Goodrum, the goal of most ECD is to cause a disruption in the communication flow of information in and out of computer systems. That being said, ECD does not permit the destruction of information or computer systems, just typically temporary blocked access (as in a DoS attack). In effect, ECD is not much different from physical civil disobedience; it has just adapted with the information culture of today.

After describing Electronic Civil Disobedience in moderate detail, the authors ask the question, can hacking be considered an act of civil disobedience? The core principles of civil disobedience consist of not causing damage to persons or property, not being violent, not being used for personal profit, being based upon an ethical motivation, and a willingness to accept personal responsibility for the outcomes.

At this point, Manion and Goodrum explain that hacktivism does fulfill the requirement of ethical motivation, as this is the foundation of activism (they provide multiple examples of hacktivism campaigns to prove this point, including quotations from hacktivist groups themselves). They also discuss a differentiation that must be made for someone to be a hacktivist. The hacker should not be an individual who attempts their exploits and infiltrations for the mere challenge or for bragging rights (this fulfills the personal profit requirement from the civil disobedience requirements). In addition, they should not be cyberterrorists, who use information technologies to wreak havoc and cause harm and/or death. Cyberterrorism is blatantly illegal and is motivated by the idea of causing damage and violence, and therefore is not a form of “civil” disobedience. True hacktivist campaigns usually accept responsibility for the outcomes of the work they perform.

The authors prove that hacktivism should be defined as Electronic Civil Disobedience per the requirements listed above. As a result, they argue that the punishments for hacktivism should reflect those of similar civil disobedience actions, rather than those of cyberterrorists (which, as will be discussed in one of the following papers, is often the case). The penalties for hacktivism are often identical to those of malicious hacking, even when no harm is done. Governments usually do not consider hacking as a political activity, and thus do not have a separate set of punishments for hacktivists. Instead, hacktivists are often labeled cybervandals or cyberterrorists, despite their civil disobedience.

This is not to say that cyberterrorism does not exist. According to Manion and Goodrum (and most everyone in today’s technological world), cyberterrorism is real and it is a significant threat. However, cyberterrorism needs to be correctly identified and not confused with hacktivism (several hacktivist groups themselves are very insistent on this distinction).

The authors then ask the question, why do experts (and the media) refuse to make the distinction between hacktivists and cyberterrorists? They speculate at the answer, but believe it may be due to fact that labeling hacktivists as criminals will help prevent others from joining the hacktivist ranks and fighting against the cooperate monopoly of the Internet. In addition, it makes it easier to erase civil rights, such as privacy, from the public, under the guise of protection and security.

Information in computing technologies creates a conundrum for those insistent on information ownership. Many hacktivists believe in the freeness of information, and therefore, they often liberate data for the rest of the world. But this is in opposition to the cooperations who want to make information a commodity and who charge for the access of data.

The authors believe that the Internet is becoming a totalitarian community, with personal liberties and freedoms being thrown aside in order to benefit the large transnational business corporations. Whether or not this is true today in 2023 is debatable, but their conclusion is valid; it appears like web freedoms are in jeopardy and as a result, tech giants want to squelch the activism campaigns of the hacktivists.

As hacktivism grows from its infancy in the early 2000s, Manion and Goodrum specify that hacktivists should fight for the core principles of the hacker's ethic (from Steven Levy): access to computers should be unlimited, information should be free, and authority/centralization must not be trusted. The principles set hacktivists against cooperations and governments and as such, the hacktivist battle will continue on for the foreseeable future. The authors call for hacktivists to take up "arms" (peacefully of course) and join the modern fight for freedom; not with the picket line, but rather online [1].

The authors do make some valid points in their discussion on hacktivism and they obviously believe in what they write. That being said, "Terrorism or Civil Disobedience" was written in 2000, over 20 years ago. Therefore, some of the specifics of what was written are no longer applicable. More current research would need to be done to discover whether or not hacktivists still follow the principles of civil disobedience.

Another side point would be, does it really matter? Sure, hacktivism is not cyberterrorism, but if it isn't right, why should we care so much about it. The authors definitely have a libertarian outlook on life, which while is exemplary at times, often can lead to the destruction of civilization if not kept in check. A libertarian Internet view has to allow for online vices such as pornography, black market transactions, and trojan horses.

One topic that was not considered in the article was that of who controls the Internet. Civil disobedience is disobedience of laws in such a way that hurts those who made the laws; however, most of the time with ECD and hacktivism, it is not the lawmakers who are suffering from attacks, but rather business and organizations who have paid a high price to have their sites on the Web.

### 2.2 Hacktivists or Cyberterrorists?

A related paper that goes a bit more in-depth in terms of examples (and personal attacks) is "Hacktivists or Cyberterrorists? The Changing Media Discourse on Hacking" by Sandor Vegh. Like the previous paper, this essay discusses the differences between peaceful activists and online terrorists (if they even exist). Once again, this paper is a bit dated, having been written soon after 9/11; however, this fact does provide an interesting perspective at some of the details concerning hacking that are often forgotten in today's society.

Rather than looking at monopolist cooperations as being the major opposition to hacktivism, Vegh takes a look at the government's role in the debate, and in turn, the media's discourse. In his introduction, the author theorizes that the government is passing restrictive legislation and is gaining public support in doing so by making hacktivists the "bad guys" and threats to our safety. In turn, the media (whether intentionally or not) plays up the vilification of the hacker and labels them as terrorists and threats to society.

Vegh points to September 11, 2001 as being a major marker in the change of the discourse on hacking and terrorism. It was a result of the terror attacks that the U.S. government introduced "protective and restrictive regulations in the name of national security." These laws threatened the liberties and freedoms enjoyed by the public, but were disguised as protections against some adversary that threatened more than constitutional rights. Cyberterrorism was getting out of hand and American lives were at stake. Or were they?

The legislation passed in the days succeeding 9/11 gave authorities the right to classify almost any hack as terrorism. As a result, hacktivists were now labeled as cyberterrorists, and even potentially cyberwarriors. Academia, activist groups, watchdog groups and more came out and advocated against the legislation that was passed to face this new brand of war on terror, but unfortunately it was not enough to stop the protective hand of Big Brother.

While this issue of hacktivism vs. cyberterrorism took a major upsurge in the post-9/11 days, it did not start there (as evidenced by the previous paper that was written before the terrorist attacks). Even in the late 90s political hacking was considered a form of cyberterrorism, cybervandalism, or malicious hacking (all of which, Vegh points out, is colorful language used to "disregard the motives and goals of online activism").

At the time of the writing, the author points out that cyberterrorism was still in the future. Sure, some attacks have caused nuisances, but they had hardly been used to wage attacks. Rather, terrorists seemed to have only really used the Internet for communications, raising funds, and spreading propaganda, none of which is illegal. So, the media had been playing up events as something that had not yet truly occurred. One reasoning behind this may be that if the government could convince its citizens that attacks were occurring, it would be easier to pass laws that fought against them; that is, fought against those who disagreed with them, but weren't actually causing harm.

The author proceeds to illustrate the media's role in this misinformation. During the 90s and early 2000s, two world leaders were supposedly using information technologies to advance their causes. One of these was the glowing picture Subcomandante Marcos, who used his laptop computer to communicate with his followers to lead the rebellion against the Mexican government. The other was horrifying depiction of Osama bin Laden using his Internet connectivity to communicate with his minions in orchestrating terror attacks. These ideas filled newspapers during a time when computing technology was gaining popularity. On the one hand, the Zapatista rebels were honored for their ingenuity in fighting for freedom, while on the other, computing technology was deemed a danger, as it was being used to take over the world.

Except neither one of these images were correct. When further investigated, it has been found that Subcomandante Marcos potentially did not use laptops and computing technologies as was advertised, and the pictures that had been painted were merely technological propaganda. Likewise, much of the information being published about bin Laden's use of technology was propaganda to inflate the dangers of the Internet.

As Vegh points out with numerous examples, the discourse on hacking by the media has been speculatory at best, and often inflates the seriousness of situations to prove whatever point is most profitable at the time. An interesting situation arises with new tools like encryption and other online communication technologies (like peer-to-peer networks and wireless networking). These technologies are problematic for the elite, as they allow for the spread of activism, while at the same time threatening the financial monopolies of those who control information. Since they threaten the current state of affairs for government and cooperations, they have been labeled as dangers and weapons of the cyberwar.

One prime example of this twisting of information is that of encryption, namely the freely available Pretty Good Privacy (PGP) protocol. Apparently, bid Laden had been communicating with his terrorists using PGP, and as such, the National Security Agency was unable to eavesdrop on their communications and in turn were unable to prevent 9/11. But there is no proof that the 9/11 used PGP at all. A similar situation occurred for Al-Qaeda's use of steganography for sending messages. Why would the media spread such unsubstantiated claims?

Even the Internet itself has fallen prey to attacks because of its hosting of terrorist organizations. In response, Vegh states that "the Internet is just like any other tool; it can be used for good as well as bad…" Ironically, it appears as if the Internet has been used for bad, just maybe not exactly in the way the media wants to admit. Rather, it has been a prime avenue for spreading misinformation and silencing opposition. And if you can silence your opponents, then they are not much of a threat.

While Vegh's article has a strong anti-government theme to it, it does cause one to consider the details concerning the government's response to 9/11. Coincidently or not, Internet freedoms were significantly restricted after the terrorist attacks on that day.

While he does not come out a directly espouse or deny it, Sandor Vegh may be a part of the 9/11 "truther" movement, which claims that the terrorist attacks were manufactured by the U.S. government. Many of these "truthers" believe that the government caused or allowed the attacks in order to make way for the legislative restrictions that soon followed. While he never explicitly discusses this idea, some of his statements seem to hint at it. For example, he never directly blames Al-Qaeda for the attacks and he discusses some statements that were made prior to 9/11 that may indicate he believes the 9/11 attacks were purposeful in order to make way for new restrictions.

In his conclusion, he does leave the option that there may not be a government agenda behind the modern discourse on "cyberterrorism", but he also mentions the fact that much of the wording in the media comes from the government. He suggests that maybe the post-9/11 legislation was really put in place to secure the country, but also counters that it has prevented political dissent, allowed for monitoring of citizens, and permitted the commercialization of information. Obviously, Vegh has a very libertarian view of the cyber-realm. While his points may be valid, and his evidence seems to be authentic, he may have taken his theory too far and connected some dots that had nothing in common [2].

What is surprising is that Vegh paper was written over ten years before Edward Snowden revealed much of the true innerworkings of the U.S. intelligence community. Had he known about dataveillance, one can only imagine how much more vocal his paper would have been.

### 2.3 Against Cyberterrorism

Unlike the two previous articles that were written in 2000 and 2002 respectively, "Against Cyberterrorism" is a more modern article, written in 2011 by Maura Conway. This difference in date is important, as this article is updated with more modern events. The first two articles suggest that cyberterrorism was a threat in the future, but this article has the advantage of being in the future (or at least 10 years in the future). As such, one would expect the predictions of future cyberattacks to have revealed themselves by now. But this is not the case, at least according to the author. The subtitle of the article illustrates this: "Why cyber-based terrorist attacks are unlikely to occur."

Conway believes, similarly to Vegh, that the media sensationalizes hacks in order to feed the fear of the public. She claims that the term "cyberterrorism" has special significance as it combines the fear of terrorism with the fear of technology; that is, the fear that technology will one day rule over humans.

The issue with cyberterrorism is that it is difficult to define. The confusion often made by people is in the difference between cyberterrorism and terrorist use of cyber systems. Those who believe cyberterrorism is imminent are labeled "Hypers", while those who deny if are "De-Hypers", which is obviously the camp that Conway finds herself in.

Conway states three reasons why she is a “De-Hyper” and why she believes, as of 2011, cyberterrorism is still a concept of the future. Her first argument against cyberterrorism is that terrorists, in general, do not have the IT experience to carry out a cyberterrorist attack. In addition, Conway argues that real-world attacks are difficult enough and that hiring third-party hackers would cause risks to the operations of the terrorist.

Her second argument is a bit more non-traditional and uncommon. She theorizes that part of the draw of terror attacks is the “Image Factor,” or the prominence of the attack based on the extensive photographic and videographic journalism (look at 9/11, for example). Cyberterrorism attacks would not produce the same result of images, as shutting down power grids and polluting water supplies hardly have much photographic appeal (one exception that Conway does point out is the potential of crashing planes through infiltrating air traffic control systems).

The third argument that Conway uses to prove cyberterrorism is not a current threat is the so called “Accident Issue.” This theory states that terrorist attacks will not occur unless the attack itself is obviously not an accident. Terrorist attacks are usually overt and purposeful, and the terror group behind it usually takes responsibility (recall that is also true for hacktivists). The goal of terrorism is to cause fear in people, but if people believe an attack was just an accident, who are they scaring? Without a second plane hitting the World Trade Center, who would have thought the United States was under attack? Everyone would have believed some horrific accident had occurred, but surely not a terror attack.

So, based on these three arguments, the author of “Against Cyberterrorism” believes cyberterrorist attacks are unlikely, especially given their high costs. In conclusion, Conway hints at the subject of some of the other papers already considered, that the media purposely inflates the dangers of hackers and keeps a close connection with policymakers.

Conway’s paper does not itself make an argument for or against hacktivism. In fact, it does not technically even mention the term. But it continues the thought process of the two previous papers, both of which place the concepts of cyberterrorism and hacktivism at enmity. However, if cyberterrorism, as Conway posits, does not exist, the two ideas cannot coincide. Therefore, in effect, if Conway’s argument is valid, Vegh’s, Manion’s, and Goodrum’s may not be (note: this is not necessarily true, it just requires an adaptation of understanding of the previous arguments) [3].

### 2.4 Hacktivism: A Theoretical and Empirical Exploration of China’s Cyber Warriors

We turn our attention back to the concept of hacktivism and what it exactly is (we have discussed plenty what it is not, namely cyberterrorism). That being said, Yip and Webber in “Hacktivism: A Theoretical and Empirical Exploration of China’s Cyber Warriors,” decide to label the Chinese hacktivists as cyberwarriors, a label that caused much chagrin to Vegh. Perhaps this is a cultural difference, but it does not seem to be derogatory toward the Chinese. Yip and Webber define hacktivism as “a phenomenon in which hacking converges with political activism.”

The main goal of Yip and Webber’s paper is to consider the hacktivist actions taken by the Chinese (many of the hacktivist campaigns across the globe had their beginnings in China). They use both a theoretical model and an empirical study to help determine some of the characteristics and patterns of hacktivism efforts across the China.

From their theoretical study, Yip and Webber discover that the main motivations for hacktivism in China are ressentiment and relative deprivation.

Ressentiment can be defined as the hate of another; it is an unrelenting, permanent feeling that something can be done that may result in action. It differs from resentment in that it is usually not temporary. Relative deprivation is the feeling of not having something when compared to someone else (basically, a severe form of jealousy). These two concepts coincide when looking at the People’s Republic of China and the government’s patriotic education campaigns used to increase the nationalism of Chinese citizens. These nationalism campaigns backfired; however, when citizens realized they were not allowed to speak against their government, as it would hamper nationalist opinions. As a result, hacktivists turned to the Internet to release their feelings of ressentiment and relative deprivation.

This theoretical discovery led the authors to suppose that whenever a political event occurred and the public became upset, there would be a corresponding surge in hacktivism membership and activity. They use their empirical study to prove this point. They decided to use online hacktivist forums and they gathered information regarding hacktivist groups that had been in operation between the late 90s and 2011. Due to lack of data and relevance of some groups, the authors focus on observing details regarding the multiple generations of the Honker Union of China, or H.U.C. (“honkers” means read hackers).

When considering the first generation of H.U.C., from 2001 to 2004, the authors found that a surge in growth occurred during June 2001. They conclude that this growth was due to corresponding world events including a collision of a U.S. spy plane and a Chinese fight in April of that year and growing conflicts between China and Taiwan (something that likely increased ressentiment in the Chinese people). This extreme growth, illustrated in Figure 1, was also due to the fact that hacktivism had become a more well-known concept and as these events transpired, interested citizens joined the ranks.

The next “generation” of H.U.C. experienced a large surge in membership in April of 2005 (a 203% increase in just 17 days). The reasoning behind this growth is posited by the authors as being due to outcries against the rewriting of history books in Japan (to omit Japanese war crimes), coupled with the public news that H.U.C. had been regrouped after its disbandment the previous year.

The authors had difficulties with the third, and final.(at least up until 2011), generation of H.U.C, as some of the information they used in the previous generations was not available, despite the presence of major political events. They determine that there were increases in average time spent on hacktivist forum sites and that the unique page views per user some significant increases, indicating the hacktivist movements were gaining in popularity.

Yip and Webber provide an alternative look at hacktivism in that they attempt to get at the root of the issue: what causes activist to take a stand. Their work is informational, but is lacking due to some absence of data. It would be an interesting experiment to continue this work and to look outside of just a single society to find data [4].

### 2.5 Investigating Web Defacement Campaigns at Large

“Investigating Web Defacement Campaigns at Large,” by Maggi, Balduzzi, Flores, Gu, and Ciancaglini, is a bit of a different style of paper then those consider so far. It is more theoretical and technical as it discusses research that the authors performed in trying to catalog and categorize campaigns of web defacement, a common type of hacktivism. Web defacement does not always mean hacktivism, but web defacement is a common tool that hacktivists use, as it sends a message without causing any real harm (as long as the defacement is not displaying pornography, downloading viruses, or causing other maliciousness).

Web defacement is the “practice of altering the web pages of a website after its compromise.” The defaced pages often provide adverse effects to the victim site. The authors of the paper found that many defacing campaigns are part of team missions and when large amounts of defaced pages are compared using machine learning, certain characteristic of them can be found and determinations can be made regarding the guilty parties and the motives behind the defacement. The number of defacements that occur every year is staggering. See Figure 2 (from [5]) that illustrates the number of defacements from 1998 to 2016.

The work done by the authors has four main contributions to the study of web defacement campaigns. First, they conduct a measurement on a dataset of 13 million defacement records. Second, they introduce an approach to identify defacement campaigns. Third, they illustrate the benefits of their approach in terms of analysis. Finally, they demonstrate, through real-world cases, how defacement is used for dark propaganda purposes.

The authors detail their process of analyzing the metadata and content of defacement records and compile a list of attributes (such as timestamp, URL, embedded resources, etc.) to use in the evaluation process. When looking at the overall statistic and trends, they found that the topical focus of defacements changed drastically over the analyzed years. Until 2005, most of the defacements exposed the lack of security in the target and illustrated how the attack was performed. In 2005, things changed and the focus of attacks highlighted world events and took stances regarding opinions of matters in the news. They also discover that the amount of malicious content found in defacements has increased dramatically from the late 90s.

Two interesting observations that the authors make are that web defacers (and in turn, many hacktivists) do not work alone. Rather, they often resemble some type of cyber gang and they often perform defacement campaigns. Consequently, many teams use campaign templates that they reuse for multiple attacks, resulting in many defacement pages being similar (or identical) to others within the same campaign.

Throughout the rest of the paper, the authors discuss their approach to analyzing defacement features, detecting campaigns, and labeling/visualizing the campaigns. The exact process is not relevant to our discussion; however, their results do provide some interesting information.

They determine that 53% of attackers are lone wolves and do not claim allegiance to any defacing team. In addition, 80% of attackers maintain their allegiance to an organization (if they are part of one) throughout their hacking careers, while the other 20% float from one group to another. Finally, 70% of defacing campaigns can be considered joint campaigns, meaning they share common goals and motives.

This data is interesting because it shows that there are variants among web defacers. Different individuals and groups operate in different ways, but their mission is usually the same: advocating for some ideology or protesting against some policy.

Web defacement is often considered a form of hacktivism; however, it does have the possibility of crossing the boundary from being annoying to being harmful. Unfortunately, this has happened with several defacement campaigns, as illustrated by several of the images in the paper. It is difficult to outright say that web defacement fits into the definition of Electronic Civil Disobedience (from [1]), but it definitely can be used in this manner. Web defacement is a common tool used in hacktivism as it gets a message across very straightforwardly [5].

## 3 CONCLUSION

Hacktivism is a complex subject that is hard to determine whether or not it is ethical or unethical. On the one hand, it is a peaceful performance of civil disobedience, in which a hacktivist demonstrates using nonviolent methods, like web defacement, to show the world his (or her) beliefs and/or ressentiment. On the other hand, hacktivists commit crimes and any society that starts making exceptions to laws will soon have a hard time stopping any crime.

A major issue among the papers considered is that of the hacktivist versus the cyberterrorist. The importance of this issue is interesting, especially considering how several of the same papers argue that cyberterrorism has not occurred yet. Regardless of whether or not cyberterrorism is a reality, the papers do prove that the discourse on hacktivism is not accurate and usually inflates the severity of the issue. That being said, hacktivism (at least Electronic Civil Disobedience) is illegal, and therefore it not as exemplary as several of the authors try to make it. out.

Should hacktivists be treated as cyberterrorists? No, they should not, as their activities can hardly be considered terrorism. Yet, they are criminal and should be prosecuted. There is a time and a place for civil disobedience (there are even positive examples of this in the Bible), but it must be done with the acknowledgement that there are consequences. And this civil disobedience should only be performed in the most extreme of cases when serious injustices are taking place, which unfortunately is not true for most hacktivist campaigns.

In general, hacktivists fight for freedom from authority, in some form or fashion. While there are times and places to advocate for one's rights, hacktivism often calls for anarchy and insubordination. But without authority, nations will collapse. Instead of campaigns of blocking sites and defacing webpages, perhaps hacktivists could turn to holding meetings and conventions where they can advocate for their rights.

In the United States of America, we have special protections under the Bill of Rights. In particular, the First Amendment guarantees the freedom of speech, the right to assemble, and the right to petition the government. These are all legal avenues of advocating for change. Perhaps hacktivists should consider trying some of the methods created for them by our Founding Fathers before going about and breaking laws.

## IMAGES

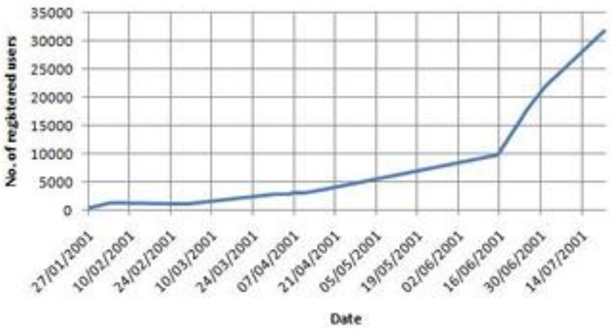

Figure 1: Membership growth of H.U.C. in 2001 [4]

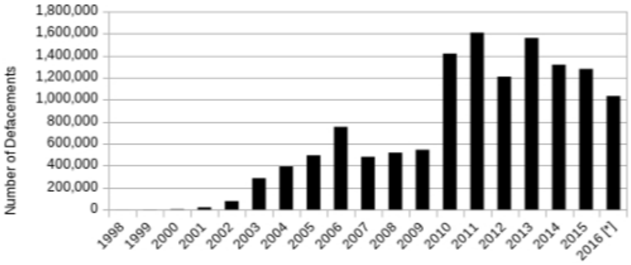

Figure 2: Records per year from Jan. 1998 to Sept. 2016 [5].

## REFERENCES

[1] M. Manion and A. Goodrum, "Terrorism or civil disobedience," *ACM SIGCAS Computers and Society*, vol. 30, no. 2, pp. 14–19, Jun. 2000, doi: https://doi.org/10.1145/572230.572232.

[2] S. Vegh, "Hacktivists or Cyberterrorists? The Changing Media Discourse on Hacking," *First Monday*, vol. 7, no. 10, Oct. 2002, doi: https://doi.org/10.5210/fm.v7i10.998.

[3] M. Conway, "Against cyberterrorism," *Communications of the ACM*, vol. 54, no. 2, p. 26, Feb. 2011, doi: https://doi.org/10.1145/1897816.1897829 .

[4] M. Yip and C. Webber, "Hacktivism: a Theoretical and Empirical Exploration of China's Cyber Warriors," Proceedings of the 3rd International Web Science Conference, 2011, doi: https://doi.org/10.1145/2527031.2527053

[5] F. Maggi, M. Balduzzi, R. Flores, L. Gu, and V. Ciancaglini, "Investigating Web Defacement Campaigns at Large," Computer and Communications Security, May 2018, doi: https://doi.org/10.1145/3196494.3196542.