Into the Grey
The Danger of Underestimating Hacktivism

Yuval Bacal

In November 2014, the hacktivist group Anonymous initiated an online campaign against the Ku Klux Klan, "unhooding" members and revealing their personal information, as well as hacking into Klan's twitter account. The attack came as a response to a Klan announcement warning people against rioting in response to an upcoming grand jury decision concerning Darren Wilson, the police officer who shot and killed Michael Brown, an unarmed black teenager, in Ferguson, Missouri. Public response on social media expressed wide support for the campaign (Altus). At first glance, this event might seem like an embodiment of civil activity, confronting an issue for the benefit of the public. However, further review raises the question: does the end really justify the means?

This article discusses the underestimated threat of hacktivism, defined as "the intentional access to a computer system and/or website, without authorization or exceeding authorized access, in pursuit of a political goal" (Maras 158). It is a unique type of cybercrime which relies on obscurity and ambiguity, first through the measures it uses, but perhaps more significantly through the issue of its legitimacy. Using various examples, the following analysis delves into the main two reasons hacktivism poses a great threat: its potential harm is vastly underrated, and there is a continuing campaign to legitimize it. Based on this discussion, the concluding portion of this article will include recommendations to further mitigate the phenomena.

Means and Ends

There are several features characteristic of cybercrimes which pose unique obstacles to governments and law enforcement agencies trying to stop them. A few of the more pernicious ones are as follows: the global interconnectedness of the internet, leading to issues of jurisdiction; the relative ease of anonymity for perpetrators; and technological advances enabling a single offender to engage in multiple offences simultaneously, reaching thousands of victims in an instant (Moitra 107-108; Cammaerts 427; Caldwell 12). The special case of hacktivism, however, adds another layer to further complicate its mitigation – its self-justification by advocating political goals "for the greater good," as opposed to personal gains that are the objective of most other cybercrimes. By attracting public support, promoting their actions as acts of civil disobedience and protest, and not seeking any obvious personal gain, hacktivists help many forget that actual crimes have been committed.

Having evolved primarily from the "hacker" community of recent decades, hacktivism – a combination of the words "Hacking" and "Activism" – is frequently associated with a political agenda that

comprises freedom of information, government and corporate transparency, and the exposure of corruption. This association has also been reinforced by the activity of the most prominent hacktivist groups in recent years, Anonymous and its offshoots LulzSec and AnonSec, who promote these principles (Kelly 1665-1666). Nevertheless, as shall be further addressed, hacktivists can act on behalf of more diverse, alternative political agendas as well – a fact that many people tend to overlook.

In his article Hacktivism: A New Breed of Protest in a Networked World, Noah Hampson (517-521) identified five main methods by which hacktivists pursue their agenda: Denial of Service (DoS), website defacements, website redirects, virtual sit-ins, and information theft. While some can be performed—or at least argued to be—under certain circumstances in a legal manner, all five include illegitimate elements and have all been illegally executed in recent years.

DoS attacks apply several means in order to block access to websites on the internet, mainly through overloading them with information requests. They are commonly applied in the form of a Distributed Denial of Service (DDoS), where the initiator of the attack controls a network of computers, called a botnet, to do his or her bidding. In most DDoS cases, the networks' "bots" are "recruited" through the use of malicious software without the knowledge, let alone consent, of their owners (Caldwell 17; Goode 77). Anonymous' 2010 attack following the WikiLeaks' funding cut offs is a good example. In early December, after WikiLeaks published thousands of the US government's diplomatic cables, Amazon, whose Web Services servers were used to run the website, decided to remove it. Similarly, companies such as PayPal, Visa and MasterCard have frozen their WikiLeaks accounts. Within days, Anonymous had retaliated and coordinated DDoS attacks against their websites, and also the websites of PostFinance, EveryDNS and MoneyBookers. Aside from Amazon, all targeted websites were forced down for a several days. Ostensibly, all DDoS "bot" computers have joined the attacking voluntarily – using a software called Low Orbit Ion Cannon (LOIC). As it turns out, many of the attacking network's bots were obtained illicitly (Cammaerts 431-432; Cadwallader).

Website defacement "involve[s] obtaining unauthorized access to a web server and either replacing or altering a web page with new content that conveys a particular message" (Hampson 519). Hacktivist targets include, among other websites, those set up by governments, law enforcement agencies, public universities, private companies and other nongovernmental organizations (Mansfield-Devine 6; Hampson 517; Maras 30). Most countries with existing cybersecurity legislation have rendered such activity illegal. For instance, the United States Computer Fraud and Abuse Act of 1984 (CFAA) prohibits "intentionally access[ing] a protected computer without authorization, and as a result of such conduct, caus[ing] damage and loss" (18 U.S.C §1030(a)(5)(C)). In the United Kingdom, the Computer Misuse Act 1990 (CMA) describes "[u]nauthorized acts with intent to impair, or with recklessness as to impairing, operation of computer" as offenses which can be prosecuted in court. The European Convention on Cybercrime, "The only international treaty to standardize cybercrime investigation, defense, and coordination tactics amongst its members" (Kelly 1686) defines in Articles 2 and 5 the actions of "Illegal Access" and "System Interference" as illegal offenses (Hampson 522).

The third and fourth common forms of hacktivism, site referrals and virtual sit-ins, are closest in essence to legal activities of protest, yet still engage in conduct that violates the rights of website owners.

In referrals, the perpetrators gain "unauthorized access to a web service and adjust the address settings", making the viewer "reach an alternative website" – usually a mock version. In virtual sit-ins, the perpetrators repeatedly reload an accessed website, either manually or by code, in order to exhaust its internet traffic resources. In this instance the question of whether the website is considered a private or a public space becomes relevant, as will be further discussed in the next section (Hampson 520).

The fifth common method of hacktivism, information theft, is probably the most harmful and widespread in practice. Unlike other cybercriminals, the information obtained by hacktivists is not kept for personal usage but is instead published for the world to see. As noted, the purpose of such action is to sway public opinion or promote a political cause, yet little consideration is given to broader implications of such activity or collateral damage which can result from the mass release of sensitive information (Kelly 1686). For example, in December 2011 LulzSec raided the servers of Stratfor Global Intelligence Service (Stratfor) and released "e-mail correspondence, financial and personal data – including 60,000 credit card numbers – belonging to 860,000 clients" (Smith). The perpetrators were concerned with exposing illegitimate public-private activities, and encouraged the use the credit cards' information for donations to charity ("Hacktivism Endures" 18). Little concern was given to the clients—often casual readers of Stratfor's reports and articles—who had been put at risk of fraud and identity-theft. Similarly, in an opposition campaign against a proposed state-bill dealing with immigrant-profiling, 700 confidential documents from Arizona's Department of Public Safety were leaked, including home addresses and social-security numbers of law enforcement officers (Mansfield-Devine 6). As a final example, in 2011 Anonymous attacked Sony's PlayStation network and released the usernames and passwords of over a million users. Consequently, Sony had to shut the network down for over a month, with losses estimated at $170 million (Cadwallader; Kelly 1665-1666).

An Underrated Threat

While the methods listed above might be described by some as relatively mild in comparison to other forms of cybercrime; it is important to remember that they represent only what has commonly been employed by hacktivists, not what the definition of hacktivism allows perpetrators to do. In fact, other forms of attack can – and according to some scholars will – be used by hacktivists leading to harsher results (Al-Rawi). In 2012, Verizon published a report claiming hacktivists have surpassed cybercriminals in the total amount of damage caused by their cyberattacks (Kelly 1707). Anonymous' attack following the WikiLeaks cutoff also included Sarah Palin's PAC and the website conservatives4palin.com (Cammaerts 432). Imagine what the consequences would have been if these attacks were to occur on Election Day. In fact, hacktivism hides a far greater potential to harm the most basic democratic process of public voting: from denying voter registries to even changing the vote tally!

In addition, some instances of information theft, once publicly released, could put individuals in grave danger. Private details of law enforcement officers could put them and their families at risk of retribution. So does the publication of snitch lists, as Anonymous did in 2011 (Kelly 1673). To take an example involving actual armed international conflict, the Syrian Electronic Army (SEA), a self-proclaimed hacktivist group who supports Assad's regime in the ongoing civil war in Syria, released private information on members of Syria's opposition groups. Anonymous, in return, published the names and details

of SEA's leading members (Al-Rawi 422-423). Both acts' victims have thus been put at greater risk for physical harm in an ongoing violent struggle that, according to some estimates, has taken the lives of over 250,000 men, women and children (Kaplan).

Popular perception of hacktivism is based more on the general familiarity with past occurrences than with the true meaning and potential it holds. As a result, hacktivism is vastly underestimated as a threat by society.

Some people would describe hacktivism as an adolescent form of more dangerous embodiments of political cybercrimes: cyberespionage, cyberwarfare and cyberterrorism. But again this perception is biased by the methods hacktivists like Anonymous have only engaged in, not by the full capacities at their disposal. When it comes to sabotaging infrastructure, for instance, there is a blurry line between hacktivism and cyberterrorism with respect to the magnitude of damage or the type of target attacked. In other words, hacktivists can damage or suspend the operations of national infrastructures in ways that do not fall under the definitions of cyberterrorism (Al-Rawi 422). Groups involved in cyberwarfare also try to hide their government affiliation and describe themselves as hacktivists. The SEA, for example, is broadly perceived to operate on behalf of Assad's government (Al-Rawi). Russia's 2008 skirmish in Georgia was accompanied by DDoS attacks on the websites of Georgia's media, banks and government. These attacks are suspected to be forms of cyberwarfare; but without Russia confirming its involvement, they can only be labeled as acts of hacktivism (Maras 153-154).

As these examples show, actors do not always engage in hacktivism in pursuit of the agenda associated with the traditional hacker community. Subject-specific groups could also attempt to steal and publish information relevant to their concerns. For example, "antipoverty activists […] could seek to publish the details of a new medicine under development by a US pharmaceutical company, with the goal of ending the firm's 'monopoly' profits and making the product more widely available." Alternatively, "antiwar groups could disclose information about a new weapons system in the hope of dissuading the United States from deploying it" (US ONCIX 11). Arab members of Anonymous repeatedly engaged in cyberattacks against Israeli websites (Al-Rawi 422-423). Even the advocates of internet freedom have been known to change their political perspectives. While Anonymous consciously did not attack media organizations – "a principle designed to avert hypocritical attacks on free expression" – its offshoot LulzSec transgressed this convention. In 2011 it targeted both PBS in the United States and the Sun in the United Kingdom. The former was attacked following the airing of a documentary "biased against WikiLeaks and [its founder] Julian Assange" (Goode 76). The latter was attacked after the exposure of News International's phone-hacking scandal (Cadwallader).

Popular perception of hacktivism is based more on the general familiarity with past occurrences than with the true meaning and potential it holds. As a result, hacktivism is vastly underestimated as a threat by society. Even the fact that other forms

of political cybercrime try to guise themselves as "merely hacktivism" does not seem to change this common perception. The next section discusses another element which enhances hacktivism's danger – the outspoken attempts to legitimize it.

The Guise of Civil Disobedience

Political demonstration is a right protected by the Fourteenth Amendment to the United States Constitution, along with the First Amendment's protection of freedom of speech. Some scholars argue that hacktivism executes the "cyber version" of the same rights, and petition for governments to recognize hacktivism as such. DDoS, they claim, is the online equivalent of sit-ins like the Occupy movement, and website defacement is parallel to spraying graffiti on a wall, which under certain circumstances is recognized as an acceptable form of civil disobedience. (Knapp; Hampson).

Usually advocates for legitimacy of hacktivism use softer definitions of what hacktivism is. Hampson (514) defines hacktivism as "the nonviolent use for political ends of 'illegal or legally ambiguous digital tools' [emphasis added]." Knapp (264-265) distinguishes hacktivism from cyberterrorism according to their respective goals: "mak[ing] a statement or draw[ing] attention to a concept" as opposed to causing serious damage. Based on such taxonomy, both argue for leniency in the prosecution of hacktivists, and the amendment of the cyber-laws to distinguish them from other cybercriminals.

In fact, on January 7 2013 Anonymous submitted a petition to the Whitehouse to officially recognize DDoS as a legal form of protest and subsequently absolve everyone indicted for this activity. The petitioners have categorized their application under issues of "Civil Rights and Liberties" and "Human Rights." It gained 6,048 signatures, meaning it didn't achieve the required amount of 25,000 signatories ("Make, Distributed,").

Nevertheless, freedom of speech and the right to protest are qualified rights (meaning, that they are not unconditional like absolute rights) and need to hold to certain restrictions. For that reason, the fact that there are differences between physical and online activity – however minute some might be – creates substantial differences in determining the specific restrictions and circumstances under which they become qualified and hence protected. In other words, greater scrutiny is required when it comes to the perception of hacktivism as merely civic disobedience.

First, protest and freedom of speech manifest in the public sphere. They are protected rights when they take place in public fora or, in some instances, on private property that is open to the public. "Occupying" someone's apartment, in contrast, is illegal, as would be the case for most privately owned properties (Hampson 527-528, 532). This becomes a key point when the discussion shifts to the internet: although the internet is accessible to almost everyone and "knows no boundaries" – with the exception of ".gov" and maybe a few other variations – websites and servers are privately owned. Thus, comparing a DDoS attack to a sit-in at the public passageway to a business is erroneous. The passageway to a website is not public either.

Second, the role of the state in monitoring and, should it become necessary, interfering in a protest is also very much different on the internet. In the physical world, a public protest is immediately noticeable, law enforcement can be called to the scene quickly and, in turn, interact directly with the perpetrators – for either mediation or sanctioning purposes. This is not the case online. A website crashing does not include a banner indicating there's an ongoing DDoS attack; it takes time to determine the

source of the problem. More importantly, what can law enforcement agencies do? If they invest their resources, they might trace after-the-fact the origins of the attack. Real-time involvement, designed to protect the victim from excessive abuse, is not possible without direct interaction with the "protesters". As examples in the previous section have demonstrated, hacktivists do at times abuse their victims beyond their political purposes. This is especially evident in the theft of private information, which in many cases does not harm the government/business attacked but their individual employees instead.

Third, claims to the legitimacy of hacktivism are often biased by the populist perception of the phenomena as influenced by the values of the original hackers' community. Their efforts to expose corruption and act in pursuit of the "greater good" are easy to identify with, leading to sympathy. Thus, the fact that the methods employed are often harmful and lead to collateral damage consequently becomes ignored. Can the above-mentioned example of Anonymous and SEA be similarly justified as civil disobedience?

Fourth, sometimes hacktivists carry an additional personal agenda for carrying out an attack on top of the political justification publicly declared. Retribution in particular is a recurring theme. LulzSec's first major attack was the publication of 40,000 emails of a man who claimed to have penetrated Anonymous' network and identified several key players (Cadwallader). The SEA hacked into the database of a Dutch website affiliated with Anonymous in response to the latter's attack on the Syrian Customs website (Al-Rawi 422). Accompanying the December 2010 attacks following the shutdown of WikiLeaks was an attack on the networks of the Swedish Prosecution Authority and a Swedish law firm in retribution for their involvement in the prosecution of sexual molestation charges filed against WikiLeaks' founder, Julian Assange (Cammaerts 432). Anonymous' "'Operation Payback' targeted the Motion Picture Association of America (MPAA) and the Recording Industry Association of America (RIAA) in retaliation for [their] attempts to take down [the copyright infringing] file-sharing site […] Pirate Bay" (Goode, 76). Along with retribution, other personal gains include fame within the hacker community through a display of technical skills (Hampson 520), or simply fun and excitement (Cadwallader).

Finally, hacktivism gets mixed with other forms of legitimate activism conducted on the internet. Mock websites, ridicule, certain forms of trolling, and the dissemination of personal information based on open-source research (Workman, Phelps and Hare 188; Kelly 1677; Knapp 266) do not breach the privacy of cyber systems and data. Dorothy Denning described these methods as normative hacktivism, as opposed to non-normative hacktivism containing the methods discussed in this article (Workman et al 188). However, the insistence on hacktivism taxonomy helps those who try to keep the lines blurred. Calling legitimate methods as cyberactivism, as opposed to normative hacktivism, would better help differentiate between the legal and illegal.

Conclusion and Recommendations

The hacking community has classically been divided into two distinct groups: white hat hackers, who point out vulnerabilities in systems and networks to their owners; and black hat hackers, who use these vulnerabilities for their personal gain (Goode 77; Young, Zhang and Prybutok 285). Hacktivism created a third type of group – grey hat hackers – as their motivations do not comply with either side of the original division (Goode 77). In fact, advocates of hacktivism tend to label them as white hat hatters, while their opponents associate

them with the opposing section (Knapp 264, 282).

Nevertheless, and despite efforts by some at legitimacy, lest we forget that most hacktivist actions are illegal (Mansfield-Devine 7). Governments and international agencies need to continue their efforts at mitigating these activities, deter "thrill seekers" from pursuing them, and remind the public of who the real victims are as a result of such illegitimate measures. "Wait until the next LulzSec," some specialists warn, "sooner or later […] they're going to cross a line" and engage in even more destructive measures than previously used for promoting a political cause (Mansfield-Devine 12).

Greater efforts should concentrate on distinguishing legitimate forms of cyberactivism from hacktivism. As has been previously noted, there are certain forms of civil disobedience that can be carried out online. Even Anonymous has sometimes chosen to employ them instead of engaging in hacktivism, as happened in Operation UnManifest. Following the 2011 Norway attacks, its members flooded the internet with fake, ridiculing versions of the murderer's manifesto – making it difficult to find the original version online (Mansfield-Devine 5). Anonymous' assistance to the protesters in Tunisia and Egypt in the "Arab Spring", as well as the 2009 demonstrations in Iran, was also legitimate: assisting demonstrators to communicate and disseminate information, as well as turning the international community's attention to the problem (Caldwell 12; Cadwallader). Thus, loud online presence, mock websites, and even politically-driven trolling and doxing should be labeled as cyberactivism and distinguished from the measures of hacktivists. A sharper taxonomy would help lift the obscurity over the legitimacy of hacktivist's actions.

The distinction between cyberactivism and hacktivism would also diminish the appeal of other forms of political cybercrime that guise themselves as hacktivism. If hacktivism becomes unequivocally illegitimate, there will be no use for perpetrators in pretending to be hacktivists. This would further assist law enforcement agencies in profiling and identifying the individuals engaged in such activities (Kelly 1710).

The multitude of examples used in this article not only show the prevalence of hacktivism, but also emphasize the variety of issues that accompany it – many due to the fact that this phenomena takes advantage of "uncharted territories." Cadwallader sums up the core of the problem: "You can't arrest an idea." However, vigilantism is not part of a secure democratic society. Hacktivism tends to target issues that are socially agreeable and that probably shouldn't have risen in the first place. Internet Service Providers (ISPs) should have removed offensive content and closed abusive accounts before they grew attention to become targets. Still, as the idiom goes, the end doesn't justify all means – a fact that hacktivism's populist agendas sometimes make us forget.

> Sometimes hacktivists carry an additional personal agenda for carrying out an attack on top of the political justification publicly declared. Retribution in particular is a recurring theme.