Destructive Activism: The Double-Edged Sword of Digital Tactics

Steven Murdoch

On April 27, 2007, a group of websites in Estonia, including those of media outlets, government ministries, and banks, went offline. For three weeks, these sites were the target of a highly effective attack triggered by the government's controversial decision to move a Soviet war memorial. Similar attacks were experienced in August 2008, targeting Georgian websites during that country's conflict with Russia over the control of South Ossetia. In both cases, the Russian government was initially blamed, but eventually it became clear that "patriotic hackers" (sometimes known has "hacktivists") were the likely culprits. While the impact of these cyber-attacks was significant, criminal attacks of even greater magnitude were commonplace on the Internet at the time and continue to be a problem. The attacks in Estonia and Georgia, however, distinguish themselves by being motivated by political activism rather than criminal intent.

So far this book has viewed the empowerment of citizens through digital means as largely positive. However, the ability of the Internet to share information, coordinate action, and launch transnational campaigns can also be used for destructive ends.

Mary Joyce, ed., Digital Activism Decoded (New York: iDebate Press, 2010), 137–148.

This chapter describes how some of the tactics adopted by digital activists have been used to disrupt communications, deface or destroy virtual property, organize malicious actions offline, and publish personal information or disinformation. Actions that cause physical harm to human beings or endanger property have yet to be engaged as a tactic of activism, but this chapter will describe how other groups have taken this route. We address physical harm in this chapter because its represents the next frontier of destructive digital activism.

We often view digital activism as a series of positive practices that have the power to remedy injustice. However, digital tools—and the very infrastructure of the Internet—are value neutral and can be used for a variety of activities. The tools and practices can thus be seen as a double-edged sword to be used constructively or destructively. This dual nature raises ethical questions that I will address at the end of the chapter.

Tactics

In this chapter, destructive digital activism is divided into five categories: blocking access; destroying and defacing virtual property; organizing malicious activity; misusing information; and attacking critical infrastructure. In each of these forms of destructive activism, the inherent capacities of the Internet are manipulated to cause harm either to persons or property. In the case of blocking access, particularly the distributed denial of service (DDoS) attack, the protocol by which information is requested from a website is misused to overwhelm the response capacity of the site's server and prevent the site from responding to legitimate requests—in effect, shutting down the site. In the case of destroying and defacing property, the server on which the website is stored is again the target of the attack, though in this case the server—which is little more than a specialized computer—is hacked in order to gain access to and vandalize the site's code.

In the case of organizing malicious activities, the infrastructure of the Internet is used to allow cooperation when more conventional means, such as meeting in person, are inconvenient or impossible. Anonymous discussion boards and encryption software help activists (who are acting in the public interest) in repressive countries to evade government surveillance; they may also be used to protect activist groups acting against the public interest, such as fascist political parties, from being regulated by the government. These technologies are, as stated earlier, value neutral and protect users regardless of motive or action.

In the opposite scenario, activists can forcibly "out" their adversaries by exposing and disseminating their personal information on the Internet. Here, the same network in which anonymous communication software operates so effectively is used to make available personal information and even misinformation. Anonymous communication software can be deployed because of the "end to end" architecture of the Internet. Within this structure, intelligence lies in the end devices, which can be rapidly upgraded with new functionality without waiting for the network to upgrade, too. This dramatically increases the speed at which new technologies can be developed, but also means that end devices are more complex and thus more vulnerable to attack. Not surprisingly, the intelligent devices at the edge of the network can be compromised by the introduction of malicious software or by hacking into the system from a remote location—two techniques for causing damage to critical infrastructure.

Just as the digital activists discussed in the rest of this book have co-opted the infrastructure of the Internet to fight injustice and defend human rights, the activists in this chapter use the same infrastructure to orchestrate attacks on individuals, institutions, and even countries. Often using software perfected by criminals, they bend the Internet to their own more sinister goals.

BLOCKING ACCESS

The primary technique used in the Estonian attacks was the distributed denial of service attack, one of the most common forms of destructive digital activism. In a DDoS attack, a large number of computers controlled by the attacker are commanded to overload a single computer with Internet traffic. Normally the computers used to execute the attack are not owned by the attacker but belong to innocent parties who have had their PC hacked into by malicious software (malware) carried by spam or downloaded unintentionally from a malicious website. This network of compromised computers, known as a "botnet," can be remotely directed to send out spam to enlarge the network, carry out DDoS attacks, or do anything else its creator wishes.

The Estonian DDoS attack was hailed as the first cyber-war, but, in fact, nation-states have been attacking the computing infrastructure of their opponents for decades using far more sophisticated techniques. What makes Estonia interesting is that the capability to carry out coordinated attacks on significant online targets was shown to be available to ordinary citizens.

DDoS attacks and botnets were first used by pranksters, in minor squabbles between geeks and as demonstrations of technical skills. Their impact on the general public was minimal. This changed when criminals moved in and decided to make money. They refined the tools, scaled them up, and made them easier to use. Criminals would attack a major website (online gambling sites were a popular target) and demand payment to stop the DDoS. This lucrative illicit business led to significant enhancements in malware technology. Once the tools and techniques were developed by criminals and became easier to use, they were adopted by activists, who chose political rather than financial targets.

Most applications used in digital activism are not created for activist purposes: Facebook groups to organize protests and smart phones to take video of police abuses are two examples of commercial software and hardware now employed for activist purposes. Software used for DDoS attacks also originated in a field outside of activism, though the purposes of development were criminal rather than commercial.

DDoS attacks also share similarities to offline protests. Rather than recruiting unwitting victims to the botnet, some activists openly solicit volunteers by stating their cause and asking for support. Those who consent can download software that will carry out the attacks on their behalf. Sometimes volunteers are simply asked to visit a particular website and click "refresh," thus overloading the website with page requests. While this type of attack doesn't cause the same levels of traffic as a bot attack, it is much harder to distinguish from legitimate usage, which, in turn, makes it harder to filter out malicious Internet traffic before it reaches the website.

DESTROYING AND DEFACING VIRTUAL PROPERTY

Other techniques activists have used to protest the actions of their target include website defacement, analogous to the vandalism that might accompany protests. Here, someone hacks into the server hosting the site and alters the content. For example, during the Georgian conflict, an activist group supporting Russia replaced the site of the Georgian Parliament with pictures of Adolf Hitler. The development of tools for hacking has followed the same pattern as that of DDoS attacks: first, these techniques were used on a small scale by geeks, then monetized by criminals, then adopted by activists. Criminal gangs would use hacked servers for hosting illicit information or to steal confidential data and sell it. Now, activists use the same tools and techniques developed by criminals for carrying out politically motivated actions.

While the Georgian and Estonian attacks were short-lived, others are part of prolonged conflict. For example, in the Israel-Palestine "Interfada" of 2000, hackers supporting both Israel and Palestine attacked the opposing government's websites. These attacks included not only spam and DDoS attacks, but also website defacement. Attacks have grown in sophistication since then and now incorporate characteristics of psychological warfare and propaganda.

ORGANIZING MALICIOUS ACTIVITY

Carrying out effective attacks of any type requires coordination. Here, the Internet also proves very useful because online forums and email offer an easy and inexpensive means to marshal forces. In addition, easily available encryption and anonymous communication software can resist surveillance, and, in practice, the sheer quantity of information flowing over the Internet is a major obstacle to effective surveillance for any but the most sophisticated intelligence services. This allows activists who are the target of surveillance, by either law enforcement or corporate security personnel, to organize while reducing the risk of their actions being disrupted; it also helps activists operating in repressive regimes but concurrently benefits criminals. Governments fear that criminals might use the Internet to evade legitimate surveillance just as activists use the Internet to evade illegitimate and politically motivated surveillance. The ability of criminals to evade conventional surveillance, like telephone taps, by communicating over the Internet has led to legislation in many countries. For example, in the United Kingdom, suspects can be forced to disclose encryption passwords. This law has been used to threaten animal rights activists found with encrypted data that the police believe might be of use in a criminal investigation if decrypted.

The Internet's usefulness in organizing with a lesser likelihood of surveillance benefits both activists and criminals. Terrorists also use websites to recruit followers and advertise training camps. In fact, the effectiveness of the Internet for the dissemination of information means that damage can be caused even without disrupting communications.

One group that uses the Internet to organize what some have construed as malicious activity calls itself "Anonymous." It has no central control; instead members self-identify and cluster around actions for which there is a critical mass of activists. While some sites dedicated to Anonymous exist, much of the discussion happens on general discussion boards. Some of their activities are restricted to the Internet, such as disrupting online services that they disagree with through DDoS attacks or by playing pranks, but they have also organized offline protests. Most notably their activism has targeted the Church of Scientology, which has been accused of financially defrauding members and harassing those who leave or criticize the church.

MISUSING INFORMATION

While the Internet facilitates open communication among activists, a dark side exists to this free flow of information: spreading disinformation and confidential material. One such phenomenon is termed the "Human Flesh Search Engine," a loosely knit group of vigilantes mobilized in the chat rooms and forums of China. In one instance, those who expressed unsympathetic and callous opinions about the tragic 2008 Sichuan earthquake, in which tens of thousands of people were killed, were harassed with emails, reported to authorities, and had their personal information published. As a consequence, one individual targeted was arrested and another was threatened with expulsion from school. Similar actions were taken against campaigners for Tibetan independence (even those living outside of China), and their families.

Animal rights activists in the United Kingdom routinely post the personal details of individuals they believe are legitimate targets. In November 2003, when the University of Cambridge was considering building a primate research lab, one group published contact details not only of those involved in animal research, but also a seemingly random collection of individuals from the computing department, including myself. Immediately, my mailbox was overloaded with messages, some polite, others abusive, until I was able to block further ones and the site containing my details was removed. In a separate action, groups of activists intimidated the management of suppliers to an animal testing laboratory, including false claims that they were pedophiles and by sending bomb threats—with the promise that these actions would continue until they shut down their business. In 2009, individuals involved in such intimidation campaigns were jailed, but shortly afterward, the judge who presided over this trial also had his home address published on an Indymedia message board. While this posting was rapidly removed, the server hosting the message board was confiscated and police arrested an administrator.

The power of blogs and forums to allow anyone to become their own media outlet is both a strength and a weakness of the Internet. Topics ignored or suppressed by traditional media can be covered, but new and minor blogs have little to lose should they publish incorrect information. Accordingly, they are often more willing to not confirm their reports and thus to spread disinformation, as was the case with the June 2009 false rumors of accidents at several nuclear power plants in Russia operated by Energoatom. A similar incident in 2007, where rumors were spread via email and SMS, resulted in panic buying of iodine pills and canned food. These are not isolated incidents—the website Snopes.com is filled with the debunking of hoaxes circulated to friends and relatives by well-meaning Internet users. Many are merely pranks, but some have political motivations.

ATTACKING CRITICAL INFRASTRUCTURE

While the Internet allows for intimidation, it cannot directly cause physical harm unless those threats are realized in the offline world. However, as the importance of the Internet in our daily lives grows, the barrier between the online and offline worlds breaks down. The examples so far have shown how an attack on an important website can halt work, how groups can organize anonymously to avoid surveillance, and how private information on the Internet can be leaked or sold. In these cases, the actual harm caused was indirect and the threat required an offline action to cause physical harm to the target. In this final category of attack, I discuss the worrying possibility that activists could interfere with critical infrastructure, causing direct physical harm.

Although activists have not yet used digital technology to cause direct physical harm, nation-states have been carrying out such attacks for some time as part of warfare. We use the term "digital technology" here to encompass the many types of tools and infrastructure that can be used to cause physical harm. In earlier decades, harmful code was loaded directly into a computer through malicious software (malware), today such code is much more likely to arrive over the Internet. In his book, *At the Abyss*, Thomas C. Reed alleged that in 1982 the CIA sabotaged software that monitored a natural gas pipeline that ran through Siberia. This software was programmed to malfunction after a specified period, ultimately causing a large explosion and significant damage. Other cyber-attacks have been carried out as part of military operations. However, these attacks required privileged access before the malware could be introduced (in the pipeline case, the software was tampered with following a tip that it would be stolen by KGB operatives). Similarly, in 2001, a former employee of a water processing plant in Queensland, Australia, used stolen software to release sewage into rivers, killing wildlife.

Nowadays, as more critical infrastructure is connected to the Internet, the need for privileged access is diminishing, opening up vulnerabilities to criminals, terrorists, and activists alike. Indeed, while examples of more recent cyber-attacks remain classified, U.S. government departments have disclosed that they regularly have their computer systems breached by foreign entities, with government intelligence agencies suspected. Given such access, officials believed attackers could seriously disrupt distribution of food and electricity.

For example, in the 2007 Aurora Experiment, security researchers hired by the U.S. government remotely took control of a generator and caused it to shake on its foundations, emit black smoke, and ultimately self-destruct. However, while criminals have the capability to execute these attacks, we have no indication that any are trying. Terrorists, who are less likely to worry about causing harm, already have effective tactics. At the moment, the tools necessary seem unlikely to fall into the hands of activists willing to use them, but it remains a possibility.

Ethical Quandaries: How Activists Justify Destructive Tactics

Throughout this book, we have described some instances of digital activism as constructive and others as destructive. This chapter in particular has made repeated ethical judgments about what constitutes "bad" digital activism. Attributing ethical value is nevertheless difficult because activism often occurs around the world's most controversial and passionately debated political and social issues: rights violations, abuses of power, and even war.

While most readers will view the actions in this chapter as unethical—a DDoS attack on a foreign government, website defacement, or harassment—it is important to acknowledge that the activists themselves believe their tactics to be justified. To give a balanced portrayal of the instances of digital activism, in this section we will look at the different justifications such activists might use for their actions: rejecting the validity of a law, weighing positive over negative effects, and rejecting the ethical legitimacy of the negative effect entirely.

Many of the tactics discussed in this chapter are illegal, especially those that adopt tools and techniques originally developed for criminal purposes. However, many activists do not see the law as a fair measurement of the ethical dimensions of their actions. For example, during the Georgian crisis, Russian activists would likely not respect Georgian laws against the defacement of government websites because these are the laws of a foreign country that the activists see as hostile to their own nation's interests. Members of the Human Flesh Search Engine might also disregard Chinese laws against harassment if they think that the bad acts of the target justified the harassment. Part of the activist identity is to challenge the status quo—this opposition can reach beyond the particular social or political cause the group is fighting to include the laws of the society as well.

A second justification for destructive digital activism is that the negative effect of the action is far less significant than its positive effect. While the animal rights activists in the United Kingdom likely recognized that the publication of a judge's home address would lead to harassment, they probably felt that the intended effect of their action—to dissuade judges from handing out tough sentences to their fellow activists—justified their action. Likewise, even though the activists of Anonymous knew the DDoS attacks of the Church of Scientology website would annoy members and nonmembers of the organization, they likely believed that the greater goal—to stop the church's alleged abuses—justified their action.

One of the most pertinent examples discussed in the context of balancing the positive and negative effects of activism is property damage. What does it matter that a government website is disabled, the participants of the Interfada might have argued, if it demoralizes the enemy and encourages capitulation? DDoS attacks, however, rarely affect only a single targeted website. When a site is disabled by overloading the server on which it is stored, the traffic of all the other sites on that server is also disrupted. Thus, a DDoS attack is likely to damage the accessibility of unrelated sites and will probably incur expenses for parties not linked to the site being targeted. As an extreme case, during the August 2009 DDoS attacks on the Twitter account of Cyxymu, a Georgian blogger, the Twitter micro-blogging site became inaccessible to all of its 30 million users.

The final justification, and the most interesting, is that the destructive act is, in fact, not a bad act at all and thus does not need to be justified. For example, many activists, particularly those with philosophical opposition to modern materialist culture, believe that violence against property (as opposed to violence against people) is not bad. These activists could thus theoretically approve of all the tactics in this chapter that do not cause physical harm to living beings. However, while the ethical cost of property damage may be subjective, the monetary cost is not. For example, the U.S. Department of Defense estimated that it has spent $100 million in taxpayers' money cleaning up after and protecting against cyber incidents.

When justifying a destructive act, activists reject a part of the rationale used to condemn their actions. They may reject the validity of the law that finds their action illegal, the premise that the negative effect of the action outweighed any benefit, or the position that the act is destructive at all. Activism often exists in opposition to the power structures that govern ethics within societies, so it is important to judge each action on its merit rather than simply accept the determinations of those in power.

Conclusion

Looking forward, the effectiveness of destructive digital activism is likely to grow as we rely on the Internet more and more in our daily lives. And, despite the inevitable lag, law enforcement's ability to catch and prosecute digital activists will also increase. Just as the tools used by activists are often driven by criminal innovation, the experience and legislative support law enforcement gains as it investigates cybercrime will help agencies track down digital activists, making such tactics a less attractive option. Technological improvements will also help resist attacks. Today, criminals and activists are often able to circumvent existing protections, but this could change. Whether we see these advances as positive or negative depends on whether we believe the initial act was justified. While these advances would help the victims of harassment, they would also remove an avenue for protest that many consider legitimate.