Combating Hacktivism

An Analysis of a Growing New Online Threat and a Corresponding Solution

Alex Banzhaf
Introduction

On January 19, 2012, the largest cyber-attack in history shut down websites for the White House, Federal Bureau of Investigation, Department of Justice, and several other major record labels and talent agencies. The culprit, an online political protest gang known as Anonymous, represents a growing threat to Internet security: hacktivist groups. To date, no law enforcement agency or polity has punished Anonymous for the January 19, 2012 attack.

In light of the technological growth and increasing global interconnectivity, legislators must acknowledge that the still unexplored frontier of cyber-attacks and hacktivism requires attention. Potential solutions must both limit the growth of hacktivist groups and educate the general public about computers and the Internet to further protect individuals online.

Part 1 of this paper introduces hacktivism and the group Anonymous’ rise to Internet prominence. Part 2 of this paper explains the Distributed Denial of Service techniques commonly associated with hacktivist groups. Part 3 of this paper proposes a two pronged solution suggestion to ameliorate hacktivism and cybercrime involving a model statute and an educational scheme.

Part 1

People have used computers for nefarious ends since before the privatization of the Internet, and while this is nothing new, recent headlines show that there has been a transition in the manner and execution of Internet crimes, all which center around one concept: “hacktivism.” Hacktivism, an obvious portmanteau of “hack”
and “activism,” is defined as the nonviolent use of illegal or legally ambiguous digital tools in pursuit of political ends.¹ Hacktivism represents a growing threat to both Internet security and impressionable young minds. Recent events show a transition toward coordinated political attacks, which in addition to the intended objectives of Internet political protest, legitimize hacktivist organizations in a manner that spawns copycats and encourages membership.

Individuals typically hack for entertainment purposes. The Max Headroom Incident, one of the more notable examples of individual, anarchist hacking behavior, showed the impact of small group of hackers. On November 22, 1987, an intruder infiltrated Chicago, Illinois television stations in a two pronged “phreaking attack.”² The still unknown intruder hijacked both a Chicago Bears highlights broadcast on WGN-TV and a Doctor Who broadcast on PBS, and showed a video of two unknown men wearing Max Headroom masks with distorted audio of seemingly random political statements and crude sexual jokes.³⁴ The flustered sports anchor, after the close of the pirated transmission, infamously declared, “Well, if you’re wondering what happened, so am I.”⁵

The efforts of individual or small group hackers seem relatively minor in comparison to an idea that has recently been introduced to the public at large: hacktivist groups. Hacktivist groups are not a new phenomenon: The Cult of the

¹ Dorothy E. Denning, Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy, GEORGETOWN UNIVERSITY, (December 1, 2012, 2:43 pm), http://www.iwar.org.uk/cyberterror/resources/denning.htm.
² Don Hayner, “2 Channels interrupted to the Max,” Chicago-Sun Times, 3, November 24, 1987. Phreaking is an offshoot of traditional computer hacking that focuses on telephone and cable attacks.
³ Id.
⁴ Video available at http://www.youtube.com/watch?v=tWdgAMYjYs.
⁵ Id.
Dead Cow, one such group, even originated as early as 1984.⁶ One group, however, has reached prominence beyond that of any other hacktivist organization: Anonymous.⁷

Anonymous is a hacktivist collective that officially began in 2003, but practically emerged as a political organization in 2008 with a video attacking the Church of Scientology.⁸ This video contained Anonymous’ mission statement:

We are Anonymous.  We are legion.  We do not forgive.  We do not forget.  Expect us.⁹

The group employs various graphics embodying the core concept of anonymity: Guy Fawkes masks, headless men, and question marks. Furthermore, the group promotes the idea of anonymity through its online website, www.anonnews.org. The website functions as a forum, but unlike traditional forums where individuals select an identifying handle and post contributions under that handle, posters generally only identify as “anonymous.”

Anonymous has staged numerous cyber-attacks since its practical debut in 2008 against organizations Anonymous politically opposes. In addition to the Church of Scientology, Anonymous also attacked the Westboro Baptist Church, a fundamentalist organization most known for anti-gay rallies at funerals, and

---

⁷ WikiLeaks is certainly more well known, but WikiLeaks’ hacktivist activities principally involve publishing government documents and not Distributed Denial of Service attack, which is the focus of this paper.
⁹ Id.
effectively removed its website from the Internet.\textsuperscript{10} Anonymous supported lesbian, gay, bisexual, and transgender communities by hacking Ugandan government websites in August, 2012.\textsuperscript{11} Anonymous even constructed a firewall that blocked Karl Rove’s alleged plans to intervene in the 2012 United States presidential election by limiting Rove’s access into voting databases.\textsuperscript{12}

While Anonymous has engaged in many more cyber-attacks and hacktivist activities than those already detailed, the watershed moment for the hacktivist organization occurred on January 19, 2012. In response to the United States Department of Justice’s and Federal Bureau of Investigation’s shutdown of MegaUpload, an extremely popular file sharing website at the time, and Congressional consideration of the Stop Online Piracy Act, Anonymous launched the self-titled “single largest attack in Internet history:” Operation MegaUpload.\textsuperscript{13}

Operation MegaUpload entailed a multi-pronged strike on numerous websites, including the United States Department of Justice, the Federal Bureau of Investigation, The White House, The Recording Industry Association of America, the Motion Picture Association of America, Broadcast Music, Inc., and Universal


Music Group. These websites were attacked by hackers worldwide, and the websites were rendered inaccessible, some for multiple days. Barrett Brown, a spokesperson for Anonymous, proclaimed the political underpinnings of the operation: “These reactions were prompted by MegaUpload going down”

Operation MegaUpload, beyond the mere shutting down of websites, had many important ramifications. Operation MegaUpload showed that hacktivism can legitimately threaten governments. In the wake of Operation MegaUpload, federal law enforcement officers feared that they could not respond to Anonymous for fear of retaliation. Officials involved with the takedown of MegaUpload were not named in press and news releases, a rare practice done due to fears of retaliation against the officials and their families. Operation MegaUpload brought to light a dangerous continuum: “The Internet is a lawless place, and we’ve seen a turning point where governments and regimes no longer have a monopoly on technology.” Simply put, governments do not control the Internet, and Anonymous, with Operation MegaUpload, demonstrated that hacktivists can exert control in cyberspace.

Operation MegaUpload, a widely publicized attack, gave Anonymous legitimacy and credibility across online communities. Anonymous has spawned

---

15 Id.
16 Id. See video in article.
18 Id.
19 Id. Tom Kellerman, Chief Technology Officer of AirPatrol, Corp., a mobile-technology company.
multiple copycat organizations.20 Perhaps more frightening is the impact Anonymous has on children, namely teenagers. The following are posts from three different individuals on the www.anonnews.org forum:

(1)
Hi all
I’m 14 years old kid who want become a HACKER, i’m from Lithuania so my native language isn’t English. I want become a HACKER because then i was just a child everybody laugh from me, I want to revenge. My mother, father laugh from me then i said that i want to become a programmer, i hate me family because they they that i’m stupid, moron...21

(2)
I’m new here and I was wondering if you have any hacking tools such as LOIC and if so can I have the download links?22

(3)
I want to help I want to learn how to hack I want to show my country that is very very small your teachings and I want to show the people what it means to be free my country is very low in the modern world (Beiruit, Lebanon) I was living in United States so I am aware of hacking. So my question is how do you hack?23

Posts like these – hardly isolated incidents – demonstrate the impact that Anonymous’ new legitimacy has on cyber culture and impressionable youth. Teenagers, upset for myriad reasons, now have a new source of illegitimate knowledge and entertainment. Worse, this source allows them to be a part of a movement where they believe they are making a difference or a political stand. Early adolescence is a dangerous period of intellectual development, and young teens are highly susceptible to negative external influences. Gang recruitment typically begins in middle school when children are between ten and 13 years old.24

20 LulzSec and LulzRaft are both loosely affiliated with Anonymous, and are responsible for many cyber-attacks of their own.
21 Available at: http://anonnews.org/forum/post/12117.
22 Available at: http://anonnews.org/forum/post/124.
23 Available at: http://anonnews.org/forum/post/447.
Thirty-seven percent of all gang members are under the age of 18. At an age where acceptance and excitement are at a premium, and Internet gang represents a frighteningly attractive option for impressionable youth.

Operation MegaUpload’s foray into the public sphere gave the organization the legitimacy to recruit new members and sabotage the development of teenagers across the globe. We are left with a situation where Anonymous has (1) flexed its cyber muscles to the extent in a manner that brought both notoriety and public support and fear in United States law enforcement and (2) established itself as a politicized Internet movement that brings in new Anonymous members without the need for specific recruiting.

Part 2

One of the principal attack methods of hacktivists worldwide is known as a distributed denial of service attack (DDoS). A DDoS, in the abstract, is conceptually rudimentary: a hacker simply overwelmms a node or connection with information beyond that node or connection’s processing ability, thereby precluding access by legitimate users. In practical application, a DDoS is more complicated, but these complications arise primarily from the victim’s side, not the attacker’s: while either a single hacker or a small group initiates and directs the DDoS, a victim must

---


defend against the overwhelming number of attacks that constitute a DDoS. As a result, a DDoS acts as an elegant, clever means of disrupting legitimate web sites and servers in a manner that places a frightening amount of power in an individual nefarious user.

A DDoS attacks a “primary victim” network using a coordinated strike from multiple compromised systems known as “secondary victims.”27 Large numbers of secondary victims attempt to access a specific web site or server to the extent that the repeated attempts knock the primary victim offline. The logic behind such an attack displays the efficacy of a DDoS: the attacker retains relative anonymity behind a wall of unsuspecting secondary victims who are actually the ones carrying out the attack on the primary victim. In choosing a DDoS attack, hackers have two principal motivations: by distributing the attack across large numbers of individuals, the DDoS is highly successful because of (1) the difficulty of programming a firewall to block such a high number of IP addresses and (2) the amplification of attack amplitude. There are two general architectures of DDoS attacks: Agent-Handler and Internet Chat Relay (IRC).

1. DDoS Attack Architectures

27 Id. at 1. This paper speaks to the idea of a DDoS as an illegal tool, but it is important to note that a DDoS can be organized by using secondary victims that a DDoS director can acquire legally. Many have alleged that the Chinese government orchestrates such attacks using systems under their control. See Fahmida Y. Rashid, “FBI to Investigate China-Based DDoS Attacks Against Change.org,” EWEEK, April 4, 2011, (December 14, 2012, 2:04 pm), http://www.eweek.com/c/a/Security/FBI-to-Investigate-ChinaBased-DDoS-Attacks-Against-Changeorg-587229/.
Agent-Handler attacks involve the same cast of characters as described above, but with different nomenclature: clients, handlers, and agents. The attacker uses client software, run by the attacker, to communicate with the rest of the DDoS attack system. The handlers are software packages that are located throughout the Internet that the attacker’s client uses to communicate with secondary victims, here the agents. The handler program is the mechanism agents use to coordinate the DDoS: an attacker can determine which agent systems are up and running, schedule a specific attack, or upgrade the software on agent computers. Typically, owners of agent computers are completely unaware that their computer is being affected. Owners of agent computers may notice some side effects of a DDoS manifesting in unusually slow network performance, a substantial increase in the amount of spam email, or the inability to access either any or a particular website. Part of the genius of the DDoS attack is that from the perspective of a user of an agent system, these manifestations of a DDoS align with commonplace IT difficulties, and thus these indications hardly sound a warning alarm. Additionally, properly coded agent software uses minimal amounts of memory and bandwidth, thus limiting the potential side effects of the DDoS on the agent computers.

---

28 Id. at 2.
29 Id.
30 Mindi McDowell, Security Tip (ST04-015) Understanding Denial-of-Service Attacks, UNITED STATES COMPUTER EMERGENCY READINESS TEAM, (last revised November 4, 2009) (November 19, 2012, 12:00 PM) [http://www.us-cert.gov/cas/tips/ST04-015.html](http://www.us-cert.gov/cas/tips/ST04-015.html). The outbound packets sent by the attacker, through zombies, occupy a major part of the processing power of an agent’s CPU and the bandwidth of the agent’s connection to the Internet.
31 Specht & Lee, supra n. 1, at 2.
An attacker can elect to use one or multiple handlers to communicate with agents.\textsuperscript{32} Attackers generally place the handler software on servers that handle large volumes of Internet traffic to further obfuscate messages between client and handlers and handlers and agents, respectively. A visual depiction aids in understanding:

Alternatively, an attacker could employ an *IRC*-based *DDoS* attack scheme. In an *IRC*-based *DDoS*, hackers eschew the handler stage of the *DDoS* and instead use Internet Relay Chat to connect clients with agents.\textsuperscript{33} *IRC*-based *DDoS* attacks carry risks and rewards for the attacker. While it is more difficult to install agent software in an *IRC* network, the large amount of legitimate everyday traffic on *IRCs* helps mask the client-agent communications.\textsuperscript{34} In *IRC*-based *DDoS* attacks, the agents are typically referred to as “zombies” or “zombie bots,” implying that there

\textsuperscript{32} Id.
\textsuperscript{33} Internet Relay Chat, in layman's terms, is a protocol facilitating instant messaging either by a group forum or by individual private chatrooms. AOL Instant Messenger is a famous first example that has now given way to more modern tools like gChat or FaceBook chat.
\textsuperscript{34} Specht & Lee, supra n. 1, at 2.
are no handlers.\textsuperscript{35} While the IRC is not directly attacking the target, it allows an attacker to co-ordinate and recruit zombies for the eventual attack. Through IRC, attackers recruit zombies either through conventional phishing methods or voluntary participation.\textsuperscript{36}

While there are a wide variety of DDoS attacks, two main classes emerge: \textit{bandwidth depletion attacks}, designed to overwhelm a victim network with unwanted traffic that blocks legitimate traffic, and \textit{resource depletion attacks}, designed to occupy a victim system’s resources to the extent that the victim is unable to process legitimate requests for service.\textsuperscript{37}

A. Bandwidth Depletion Attacks

Within the category of bandwidth depletion attacks exist two specific types of attacks: (1) flood attacks and (2) amplification attacks. In a flood attack, an attacker, either using handlers or zombies, congests a victim’s network with IP traffic.\textsuperscript{38} The victim network connection, with only a finite amount of bandwidth capability, will be flooded with zombie traffic to the extent that the network crashes or slows to the extent that access is impracticable. Both outcomes limit a legitimate user’s ability to access the victim network.

There are two possible mechanisms by which attackers can overwhelm a victim’s network in a flood attack. The first, a \textit{User Datagram Protocol} (UDP), involves zombies sending a victim network large numbers of UDP packets that force

\textsuperscript{35} Id.

\textsuperscript{36} See Part 2, §2 DDoS Preparation Methods for more on voluntary participation.

\textsuperscript{37} Id. at 3.1

\textsuperscript{38} Id.
the victim network to process, beyond the network’s limitations, the incoming data packets to determine which applications requested data. Hackers spoof the IP addresses of the agents to further protect their anonymity: the victim system’s return packets are then sent to spoofed addresses and not the actual agent IP’s.

The hacker’s toolbox also contains TCP-based attacks, specifically SYN flood attacks. TCP connect to servers using the “TCP three-way handshake,” a three step process where: (1) the client sends a synchronize (SYN) message to a server, (2) the server acknowledges the request by sending an acknowledge signal (SYN-ACK) back to the client, and (3) the client responds with an acknowledge (ACK) signal. The SYN flood attack operates by omitting the third step, leaving a server waiting for an acknowledgement that will never come, thereby binding server resources to useless protocols.

Alternatively, a hacker could use an IMCP flood attack. The difference between an IMCP flood attack and a UDP or TCP attack is that instead of sending an overwhelming amount of information, a hacker requests an overwhelming...

---

39 Id. Transmission Control Protocol (TCP) is the most common Internet protocol. TCP is “safer” than UDP as TCP employs a flow control process that determines when data must be resent, which stops sending additional packets until previous packets are successfully transferred. UDP differs in that there is no flow control fail safe. UDP is therefore a faster, albeit less accurate, Internet protocol, typically employed in streaming media due to its speed. See Erik Rodriguez, “TCP v. UDP,” SKULLBOX SCHOOL FOR INFORMATION TECHNOLOGY, November 28, 2012 (December 15, 2012, 1:00 pm), http://www.skullbox.net/tcpudp.php.

40 IP spoofing is a technique where a hacker creates a forged IP address that does not correspond to the actual computer involved. IP spoofing could be analogized with sending a letter with a false return address to conceal the original sender’s location.


42 Id. Alternatively, the hacker can spoof the SYN IP, thus creating a scenario where the server sends a SYN-ACK to an imaginary source that will obviously not return the ACK.

43 Id.
amount of information. The requests saturate the victim network, accomplishing the same function as a UDP attack or SYN flood but with a different mechanism.

B. Resource Depletion Attack

A DDoS attack may also function as a resource depletion attack, where the goal is to send victim networks packets that are intentionally malformed or misuse protocol communications. Two sub attacks exist within the realm of resource depletion attacks: (1) protocol exploit attacks and (2) malformed packet attacks. Protocol exploit attacks, similarly to IMCP flood attacks, overwhelm a server with Transfer Control Protocol requests from zombies with spoofed IP addresses. Victim servers struggle to return the requests to the correct address and soon run out of memory resources to respond to legitimate users. In malformed packet attacks hackers, rather simply, have agents send packets that either (1) have the same source or destination IP address or (2) have randomly generated, nonsensical IP addresses. The result is the same: the victim server fails to process the bogus IP addresses and bandwidth capability is compromised.

2. DDoS Preparation Methods

44 The hacker would send high volumes of “IMCP_ECHO_REPLY” packets to ping the victim system.
45 Id. at 3.2. While this paper organizes DDoS attacks as either Bandwidth Depletion or Resource Depletion, there are other possible organizational structures. For example, DDoS attacks could be classified based on the “OSI Stack.” The OSI Stack is a method of hierarchically organizing communication systems online. There are seven OSI layers: (1) physical, (2) data link, (3) network, (4) transport, (5) session, (6) presentation, and (7) application. Various DDoS attacks target different OSI stack levels: IMCP attacks occur at the network layer, UDP and TCP attacks occur at the transport layer, and resource depletion attacks occur at the application layer. The most important principle to glean from the various classification of DDoS attacks is that a DDoS does not manifest as solely one attack method: DDoS attacks are varied in style and application, further complicating protective solutions.
46 Id. Protocol exploit attacks manifest as either “TCP SYN attacks” or “PUSH + ACK” attacks.
47 Id. These attacks are known as “IP address attacks” or “IP Packet Options” attacks, respectively.
Irrespective of what type of DDoS a hacker plans, all require one key element: an agent computer, either under the control of a handler or acting as a zombie, unknown to the legitimate user, previously installed attack code. A hacker can choose one of two strategies to implement this integral component: an *active agent installation* or a *passive agent installation*.\(^\text{48}\)

Active agent installation involves a hacker attempting to personally install DDoS software. An active agent installation involves a three part process: (1) finding and scanning systems for vulnerabilities, (2) running programs to exploit these vulnerabilities to gain access to zombie computers, and (3) surreptitiously installing agent software.\(^\text{49}\) The first part requires hackers to run a program that scans for potential zombies. Programs, such as Nmap, allow hackers to scan a particular network to determine if that network’s router implements a protective firewall, and if so, how private IP addresses are assigned within the network and what applications run on the computers behind the router.\(^\text{50}\) After compiling a list of systems, hackers then choose a vulnerability to exploit to gain access to the potential zombie. The resources available online for finding potential vulnerabilities are nearly limitless: for example, the Common Vulnerabilities Exposures organization publishes lists of thousands of different known vulnerabilities.

---

\(^{48}\) Id. at 4.

\(^{49}\) Id. at 4.1.

\(^{50}\) NMAP.org (November 20, 2012, 5:25 pm), [http://nmap.org/book/man.html#man\_description](http://nmap.org/book/man.html#man\_description). Nmap, ironically, is designed as a tool to audit systems for vulnerabilities to later protect and correct. This resource is freeware and available to anyone. Moreover, the above link provides a tutorial for how to use the product.
vulnerabilities for different types of systems. While intended as a resource for network administrators to develop security protocols, the CVE list simultaneously provides hackers with ideas for how to access and recruit zombies for DDoS attacks.

Alternatively, a hacker may attempt a passive agent installation, where a hacker attempts to have a secondary victim unknowingly install the DDoS software themselves. There are a number of methods of passive installation, but all carry the same general principle: fraudulently convince a legitimate user to, ironically, actively engage in acquiring agent software. Hackers may elect to use many different strategies, among which are the popular (1) corrupted file or (2) bugged website.

A corrupted file appears to the user to be a benevolent file, but in fact contains code that, upon viewing or executing, will infect a system with agent software. An unsuspecting user would download a text file that appears to the user to look like:

```
funnyjoke.txt
```

However, that is an illusion created by the graphical user interface of the operating system, and the actual file’s name is extended:

---

51 Common Vulnerabilities and Exposures: the Standard for Internet Security Vulnerability Names, (November 20, 2012, 5:33 pm), http://cve.mitre.org/. The “CVE” list is also freeware and accessible by anyone. The number of known vulnerabilities is nearly limitless. IBM’s Power 5 Service Processor was found on December 12, 2012 to contain a vulnerability that allows attackers to operate with elevated privileges. See http://www.kb.cert.org/vuls/id/194604. A D-Link DSL 2730U router was found to contain a vulnerability that would allow an attacker to chain unauthorized commands through authorized commands. See http://www.kb.cert.org/vuls/id/876780. It is important to note that identification of these commands does not necessarily imply a corresponding solution.

52 Specht & Lee, supra n. 1, at 4.2.

The above is intentionally extended to over 150 characters, as hackers have learned that at the 150 character mark, Microsoft Windows displays a condensed file name, thereby tricking the user. After clicking on a file, the user may very well see a funny joke; however, that joke is a façade for a different executable program operating in the background, and most likely unbeknownst to the reader, the joke file is also installing agent software for a future DDoS.

Hackers also employ phishing techniques to install passive agent software. “Bugged websites” that exploit vulnerabilities in web browsers are one example of phishing. A hacker creates a website that, upon a potential zombie’s viewing, indirectly downloads and installs agent software. Conversely, hackers also employ semantic attacks that operate by manipulating a human’s interaction with the Internet. Instead of focusing on confusing a computer, semantic attacks use social engineering to convince a legitimate Internet user to access a website under false pretenses. A bugged website can also be semantic attack, although the goal is to convince a user to directly download a file containing malicious code instead of flummoxing a web browser and installing code surreptitiously. However, the

54 Id. The comedians listed are solely for the purpose of extending the filename.
55 “Phishing” is defined as the act of requesting confidential information over the Internet under false pretenses in order to fraudulently obtain credit card numbers, passwords, or other personal data. The America Heritage Dictionary of the English Language, Fourth Edition. Houghton Mifflin Company. (2004). Contextually, phishing refers to a hacker stealing the credentials of a potential zombie in order to load agent software.
56 Specht & Lee, supra n. 1, at 4.2.
58 Id.
predominant semantic attack is a spoofed email, where a seemingly innocuous message in fact steals passwords or credentials.\textsuperscript{59}

In addition to active and passive agent installations, hackers increasingly recruit zombies \textit{willingly}. Modern DDoS hackers employ a program called the “Low Orbit Ion Cannon.”\textsuperscript{60} The idea behind the Low Orbit Ion Cannon (LOIC) is that it allows users to participate in hacks even if they know nothing of hacking and computers. A user voluntarily downloads and executes the LOIC program, and in doing so, gives a central hacker access to their computer for the purposes of a denial of service attack.\textsuperscript{61} The LOIC is simply a popular software with a “brand name” that allows unwilling Internet users contribute to an attack that they either agree with from a political standpoint or simply enjoy from an entertainment perspective.

\textbf{Part 3}

Governments, companies, and individuals generally are not without legal tools to defend against hacktivist DDoS threats. While individual attacks are already criminalized under the Computer Fraud and Abuse Act, this statutory scheme is not a sufficient protection in light of the rapid development of Anonymous, and its copycats, and the increased prevalence and popularity of Distributed Denial of Service attacks. This article suggests a two pronged solution in an effort to increase public awareness of these timely, dangerous threats: (1) an

\textsuperscript{59} L. James, \textit{Phishing Exposed} (2005).
\textsuperscript{60} Available for freeware download at http://sourceforge.net/projects/loic/.
Internet Gang Statute targeted at criminalizing illegal Internet activity done as a collective and (2) an educational platform designed to increase individual’s knowledge of computers and the Internet in the short term and to foster an encouraging, legal environment for computer learning in the long term.

1. The Internet Gang Prevention Act

The following is a model statute that could be employed at either the state or federal level. The statute is intended to effectuate the following: (1) criminalize hacktivist groups by increasing statutory penalties for crimes committed as a collective based upon pre-existing gang statutes, (2) criminalize the recruitment of agent or zombie computers typically seen in DDoS attacks, (3) criminalize specific recruitment of hacktivist members, and (4) enforce further compliance with the education reforms suggested later as the second of the two pronged defense against hacktivism and DDoS attacks.

A. Language

The Internet Gang Prevention Act

§ 1: Internet Gang Members
An “Internet gang member” is a person who meets two or more of the following criteria:
(a) Admits to Internet gang membership;
(b) Is identified as an Internet gang member by a family member;
(c) Is identified as an Internet gang member by a co-conspirator or co-gang member;
(d) Self-identifies as an Internet gang member by username, handle, ID, or account name;
(e) Self-identifies as an Internet gang member via social media statement;
(f) Is identified as an Internet gang member by physical evidence;
(g) Has been observed in furtherance of an Internet crime as a part of an Internet gang; or

62 See § 3(a)(2) for this analysis.
(h) Associates with one or more known Internet gang members.

§ 2: Internet Gang Recruitment
a. A person commits the offense of Internet Gang recruitment by knowingly soliciting, inviting, encouraging or otherwise involving a once unaffiliated person with a gang to commit imminent Internet Gang crimes.
b. An offense under §2(a) is punishable by 1-2 years imprisonment.

§3: Internet Gang Crime
a. A person commits the offense of an Internet Gang crime for committing any statutory crime involving a computer and the Internet while a member of a group with five or more members which promotes, sponsors, condones, assists in, or actively participates in the commission of Internet and computer related felonies, with knowledge of the group’s criminal purpose, and has specific intent to further the group’s criminal purpose.
b. In addition to the statutory penalty for the individual offense, an offense under § 3(a) is additionally liable for between 2-5 years imprisonment.

§4: Failure of Individual to Comply with 34 CFR X
If a person is liable under §2(a) or §3(a) and has failed to comply with 34 CFR X, that person is additionally liable for 1-2 years imprisonment.

§5: Failure of School to Comply 34 CFR X
If a person is liable under §2(a) or §3(a) and that person’s secondary school or high school has failed to comply with 34 CFR X:
1. If a teacher failed to comply with Department of Education Regulation XYZ, that teacher is subject to discipline by either (a) losing his or her teaching license or (b) a $10,000 statutory fine.
2. If a school failed to comply with Department of Education Regulation XYZ, that school is subject to discipline by $25,000 statutory fine.

§6: Civil Remedies
1. Individuals may bring private rights of action for violations of § 2, 3, 4, or 5 of this act.
2. Successful private rights of actions under §6(1) include damages including attorney’s fees.

B. Sample Models

This model statute is based in part on pre-existing language from the following state gang statutes: the Idaho Criminal Gang Enforcement Act, Ohio’s

---

63 See infra § 3(b)(i).
64 IDAHO CODE ANN. § 18–8501 (2006).
“Criminal Gang Activity” statute,\textsuperscript{65} Indiana’s Criminal Gang Control Act,\textsuperscript{66} and Florida’s Criminal Gang Prevention Act.\textsuperscript{67} Two important questions derive from these model statutes: (1) whether the statute would best function as a state or a federal law and (2) whether such a law is constitutional.

i. State v. Federal

The aforementioned statutes operate at the state level. The model statute would be the most effective at the federal level due to the geographical differences between ordinary gangs and Internet gangs. In \textit{Helton v. State},\textsuperscript{68} James “G-Dog” Helton was second in command in the gang “Imperial Gangster Disciples.”\textsuperscript{69} In 1991 and 1992, G-Dog participated in the initiation of two new gang members in Morgan County, Indiana: G-Dog performed a “46”\textsuperscript{70} on a new initiate and forced a new initiate to recite the “initiation prayer”.\textsuperscript{71} The State of Indiana prosecuted Helton under the Criminal Gang Control Act for participating in a criminal gang.\textsuperscript{72}

In \textit{State v. Manzanares},\textsuperscript{73} the State of Idaho charged Simona Manzanares under the Criminal Gang Enforcement Act with illegal recruitment of gang members.\textsuperscript{74} Manzanares admitted to being a member of the East Side Locas, a local gang in Caldwell Idaho that funds its nefarious activities by acting as local

\textsuperscript{65} OHIO REV. CODE ANN. § 2923.42 (West 2007).
\textsuperscript{66} IND. CODE § 35-45-9-1 (2007).
\textsuperscript{67} FLA. STAT. ANN. § 874.01 (West 2008).
\textsuperscript{69} 642 N.E. 2d at 504.
\textsuperscript{70} A “46” involves gang members hitting an initiate forty times in the head and six times in the chest surrounded by various gang paraphernalia. Id.
\textsuperscript{71} “Let it rain, let it pour, let a G [IGD] kill a Lord [Vice-Lord, a rival gang].” Id.
\textsuperscript{72} Id.
\textsuperscript{73} State v. Manzanares, 152 Idaho 410 (2011).
\textsuperscript{74} 152 Idaho at 415.
narcotics dealers, burglarizing local Caldwell homes, and stealing local Caldwell cars. In addition to satisfying gang membership, Manzanares demonstrated recruitment by posting an online video encouraging listeners to take part in the East Side Locas gang activities generally, specifically, “tagging.”

Both Helton and Manzares demonstrate the efficacy and intent of the statutes involved from the regional or local level. Gangs, especially gang crimes, as the facts of both cases illustrate, typically require geographical proximity between the gang members. By contrast, hacktivist attacks only require a computer with the Internet access, and as a result, not only is geographical proximity not a prerequisite for Internet gang activity, but employing such a mindset would demonstrate a fundamental lack of understanding of computer crimes from a policy point of view.

In United States v. Collins, law enforcement took its biggest stand against hacktivism to date. On January 27, 2011, the FBI, with the help and insider information of Lulzsec leader Hector “Sabu” Xavier Monsegur, executed twenty-seven search warrants in twelve different states and the District of Columbia as part of an investigation of DDoS attacks committed against Paypal in “Operation Avenge Assange.” These states included suspects in Alabama, Arizona,
California, Colorado, Florida, Massachusetts, Nevada, New Mexico, and Ohio, as 
well as the District of Columbia.  

A juxtaposition of Collins with the state gang law cases clearly shows that 
any statute focused on limiting cybercrime must exist at a federal level. One of the principal strengths of local law enforcement is its organization on a local basis. However, that localization principal is also one of the weaknesses of state law enforcement: criminal investigation is principally the responsibility of the state in which the crime occurred, and when the crime or criminal extends beyond the state’s borders, states often require assistance from federal law enforcement. By contrast, federal law enforcement and statutes derive from the notion that the United States requires an oversight body to regulate crimes occurring over broad geographic areas. Statutes such as the Electronic Communications Privacy Act and Computer Fraud and Abuse Act, both which are federal statutes that deal with the issue of technological crimes spread across state borders, demonstrate the legislative rationale that intangible computer crimes often occurring across state lines are best dealt with at the federal level.

ii. Constitutional Concerns

82 Id. at 701.
83 Sara Sun Beale, Federalizing Crime: Assessing the Impact on the Federal Courts, 543 ANNALS AM. ACAD. POL. & SOC. SCI. 39, 41 (1996). The first federal criminal law, the 1872 mail fraud statute, specifically dealt with crime spread across state borders. The growth of interstate commerce, through railroad, resulted in more need for federal criminal laws: for example, interstate transportation of cattle carrying contagious diseases was criminalized because the problem could not be dealt with adequately by local law enforcement.
The four statutes used in developing the model all had to withstand constitutional challenges.\textsuperscript{86} Analysis of the challenges involved shows that a correctly drafted statute can avoid possible constitutional concerns.


In *Helton*, the defendants argued, *inter alia*, that the Gang Statute infringed on the defendant’s right of association guaranteed under the First and Fourteenth Amendments of the U.S. Constitution by criminalizing membership within a criminal gang.\textsuperscript{87} Specifically, Helton argued that he was prosecuted for merely associating with a group of juveniles that the statute deemed a “criminal gang.”\textsuperscript{88}

The key delineation that *Helton* makes between the statutory language and the defendant’s argument is the second step required for one to be liable under the Gang Statute. Mere association *was not prohibited* under the statute: instead, the defendant must, in addition to participating actively and associating with the criminal gang, “promote[s], sponsor[s], assist[s] in or participate[s] in...felonies or batteries” before becoming liable under the statute.\textsuperscript{89}

By contrast, a similar statute in Florida was ruled unconstitutional in *State v. O.C.*\textsuperscript{90} *O.C.* involved the State of Florida’s appeal to the Florida Supreme Court that § 874.04 of the Criminal Gang Enforcement and Prevention Act was in fact

\textsuperscript{86} See supra notes 36-39.
\textsuperscript{88} Id.
\textsuperscript{89} Id. See also State v. Stallings, 153 Ohio App. 3d 5, 12-13 (Ohio Ct. App. 2002)(holding R.C. 2923.42(A) constitutional as it does not criminalize mere membership but instead requires also that a defendant knowingly participate in criminal gang conduct).
\textsuperscript{90} 748 So.2d 845 (Fla. 1999).
The Appellate Court deemed that enhanced penalties based on O.C.’s membership in a criminal street game were unconstitutional as it punished mere association. The State of Florida appealed, arguing that the Criminal Gang Enforcement and Prevention Act was constitutional. The Florida Supreme Court agreed, noting that § 874.04 differed from properly constructed gang membership statutes in that §874.04 actually did punish mere association, as the language did not provide a sufficient nexus between the gang membership and the crime committed. As written, the statute would have punished a gang member, who independently elected to shoplift for his or her own personal purposes and completely independent of gang membership, would face an increased statutory penalty, which the Court deemed an unconstitutional offense.

Thus, the principle derived is “association plus” is constitutionally valid for statutes criminalizing gang membership. As explained by O.C., membership in a gang is not a legitimate basis for increased criminal penalties unless the crimes committed relate back to the gang. The “plus” prong must create a nexus between the criminal activity and the participation in the gang and the furtherance of the gang’s criminal purpose. This paper’s proposed statute avoids this problem by only allowing for increased statutory penalties if the crime committed was done to further the Internet gang’s agenda.

---

91 Id. at 950.; § 874.04 states: Upon a finding by the factfinder that the defendant committed the charged offense for the purpose of benefiting, promoting, or furthering the interests of a criminal gang, the penalty for any felony or misdemeanor, or any delinquent act or violation of law which would be a felony or misdemeanor if committed by an adult, may be enhanced. FLA. STAT. ANN. § 874.04 (West 2008)(emphasis added).

92 State v. O.C., 748 So.2d 845, 949-50 (Fla. 1999).

93 Id.

94 See supra, Part 3, §1(A).
Gang recruitment provisions also pose constitutional questions about the right of association. In *Manzanares*, the defendant argued that the “Recruiting Provision” of the Idaho Criminal Gang Enforcement Act violated her First Amendment rights.\(^95\) The defendant cited a line of United States Supreme Court cases that placed penalties or restrictions on members of the Communist Party that, synthesized, generally hold that a statute is constitutionally overbroad if it criminalizes merely joining, participating in, or being a member in an organization.\(^96\) The *Manzanares* court noted that the cases cited do not definitively state that any and all recruitment statutes are constitutionally overbroad, and that specifically narrow drafting can create a valid law. Based on this general principle, the Idaho Supreme Court upheld the Recruiting Provision.\(^97\) Specifically, the Court drew the following distinction: while criminalizing mere gang membership recruitment for membership purposes is not constitutionally legitimate, recruiting gang membership recruitment for the purposes of knowingly and actively promoting or assisting in the commission of a gang crime is sufficiently narrow to avoid constitutional challenge.\(^98\) The principle divined is similar syllogistically to the above membership principle: criminalizing mere recruitment is constitutionally invalid, but “recruitment plus” is constitutionally valid, where “plus” refers to

\(^95\) State v. Manzanares, 152 Idaho 410, 424 (2011). Specifically, the defendant challenged the “Recruiting Provision” that states that a person commits the offense of recruiting a criminal gang member by “[k]nowingly soliciting, inviting, encouraging or otherwise causing a person to actively participate in a criminal gang.” IDAHO CODE ANN. § 18–8504(1)(a) (2006).


\(^97\) Manzanares, 152 Idaho at 425.

\(^98\) Id. For example, inviting a motorcyclist to attend a lawful Hell’s Angels rally is constitutionally protectable, but inviting a motorcyclist to ride alongside a van carrying narcotics for the purposes of distribution carries no constitutional protection.
recruiting with the knowledge that the recruit would participate in a gang crime. Manzanares demonstrated recruitment plus by specifically recruiting new gang members to engage in illegal tagging.\(^9^9\)

b. Freedom of Speech Concerns

In *Enoch v. State*, a defendant charged under the Florida Criminal Gang Prevention Act argued that §874.05(1) was unconstitutional under the First Amendment for violating freedom of speech.\(^1^0^0\) The *Enoch* court determined that because §874.05(1) was a content-based regulation strict scrutiny was the appropriate standard of constitutional review.\(^1^0^1\) The Florida legislature, in enacting the law, addressed the issue of “fighting the scourge of gang-related criminal activity,” which was a sufficiently compelling interest under strict scrutiny.\(^1^0^2\)

More analytically interesting, however, was the discussion of narrow tailoring. Agreeing that the language of “intentionally causes, encourages, solicits, or recruits” carried sufficient knowledge that membership in a gang is conditioned on imminent commission of gang related crimes to satisfy the need for intent or

---

\(^9^9\) Id.
\(^1^0^0\) *Enoch v. State*, 95 So.3d 344 (Fla. Dist. Ct. App. 2012).
\(^1^0^1\) *FLA. STAT. ANN.* § 874.05 (1) (West 2008). §874.05(1) holds: “a person who intentionally causes, encourages, solicits, or recruits another person to become a criminal gang member where a condition of membership or continued membership is the commission of any crime commits a felony of the third degree, punishable [according to punishment statutes].”
\(^1^0^2\) 95 So.3d at 350.
\(^1^0^3\) 95 So.3d at 350-51.
\(^1^0^4\) Id. See *FLA. STAT. ANN.* § 874.02(2) (West 2008) (acknowledging “a mounting crisis caused by criminal gangs whose members threaten and terrorize peaceful citizens and commit a multitude of crimes.”)
mens rea, the question next moved to whether the statute was overbroad by reaching a “substantial number of impermissible applications.”

In order for the penalty for the type of speech criminalized §874.05(1) to be constitutionally legitimate, the Court determined it must have a sufficient nexus with criminal conduct. The Court examined Brandenburg v. Ohio\textsuperscript{106}, a case involving a Klu Klux Klan film depicting derogatory comments about Jews and African Americans with the message that members needed to retake the United States government in order to “bury” non-Caucasians.\textsuperscript{107} From this, the United States Supreme Court divined the following principle:

> The constitutional guarantees of free speech and free press do not permit a State to forbid or proscribe advocacy of the use of force or of law violation except where such advocacy is directed to inciting or producing imminent lawless action and is likely to incite or produce such action.\textsuperscript{108}

The key to this principle lies in the word imminent. In Brandenburg, the potential harm was indefinite and abstract, as there was no proscribed time period for the retaking of the government and subsequent genocides, and thus the statute was unconstitutionally overbroad.\textsuperscript{109}

In Enoch, the statute covered speech that inherently implied imminence. As the Florida Criminal Gang Prevention Act defined gang membership as “membership plus,” any recruiting speech necessarily transitioned into lawless action. Therefore, the Florida Supreme Court upheld §874.05(1) as sufficiently


\textsuperscript{107} 395 U.S. at 445-46.

\textsuperscript{108} Id. at 447.

\textsuperscript{109} Id. at 448-49.
narrow, demonstrating that gang statutes are constitutional so long as they are drafted with intent and imminence in mind.\footnote{Enoch, 95 So.3d at 355.}

2. Public Education

This proposed Department of Education Regulation has two stated purpose: (1) creating an environment that encourages legitimate computer and Internet learning instead of vigilante learning through hacktivist groups and (2) increasing general computer and Internet literacy education in the United States.

A. Language

\textbf{TITLE 34 – EDUCATION} \\
\textbf{SUBTITLE A – OFFICE OF THE SECRETARY, DEPARTMENT OF EDUCATION} \\
\textbf{PART X\textsuperscript{111} – COMPUTER AND CYBER LITERACY}

\textit{34 CFR X}

a. “Computer and/or Internet Literacy”, “Computer skills,” or “Computer Sciences” may be considered a “core academic subject” under PL 107-110, Title II Part A §2101.

b. Addition of “PL 107-110, Title II Part A §2102(4)(c)”: successful completion of basic computer and Internet skills examination.

c. As a requisite for public secondary school or high school graduation, a student must complete and pass the standardized computer and Internet literacy examination during the fourth or final year of high school or secondary school education.

d. As a requisite for public secondary school or high school graduation, a student must complete and pass a standardized computer and Internet literacy course for 1 credit hour, 1 semester, or the functional equivalent, during the first year of high school or secondary school education.

B. Teacher education/certification

The No Child Left Behind Act\footnote{No Child Left Behind Act of 2001, Pub. L. No. 107-110, 115 Stat. 1425 (2002) (codified as amended at 20 U.S.C.A §§ 6301 – 7546) (2002))} (NCLBA) requires that secondary or high school teachers must be highly qualified.\footnote{X represents a placeholder given the large number of proposed regulations.} A highly qualified teacher must have at
least (1) two years of experience in a classroom and (2) postsecondary education or
demonstrated competence in a field or academic subject for which there is a
significant shortage of qualified teachers. Many of the goals of NCLBA focus on
improving student competence in “core academic subjects,” but the Act does not
outline what subjects constitute core academic subjects, as that is a state decision.
States do not include computer classes under core academic subjects. 34 CFR X
(a) would include the area of computer skills, literacy, and science as a core
academic subject that new teachers gain qualification for to satisfy the “highly
qualified” component of NCLBA.

C. Class Curriculum and High School Graduation Requirement

NCLBA includes the “We the People Program.” This program calls for
federal grant money to provide “a course for instruction on the basic principles of
the Nation’s constitutional democracy and the history of the Constitution of the
United States, including the Bill of Rights.” 34 CFR X(d) would mimic this section
in practical application, except provide for a one semester or one credit hour class

113 § 1119(a)(1), 20 U.S.C.A at § 6319.
114 § 2102(4)(c), 20 U.S.C.A at § 6602.
115 See e.g., § 1119(a)(1), 20 U.S.C.A. at § 6319.
116 See e.g., Illinois: science, music and visual arts, reading or language arts, English, history,
economics, civics, geography, foreign language, and mathematics. Requirements for Being
Considered Highly Qualified, ILLINOIS STATE BOARD OF EDUCATION, (December 1, 2012, 2:26 pm),
http://www.isbe.net/certification/html/hq_requirements.htm; California: English, reading/language
arts, math, science, foreign language, civics/government, economics, arts, history, and geography.
Subject Matter Authorizations, COMMISSION ON TEACHER CREDENTIALS, (December 1, 2012, 2:26
pm), http://www.ctc.ca.gov/help/supplement-SMA/SMA.html; Maryland: Art, music, dance, or theater
arts, social studies, civics, government, history, geography, economics, English, reading or literature
skills, mathematics, science. Core Academic Subjects, MARYLAND STATE DEPARTMENT OF EDUCATION
(December 1, 2012, 2:33 pm), http://www.marylandpublicschools.org/MSDE/programs/esea/docs/TQ_Regulations/core_subjects.htm

117 § 2344, 20 U.S.C.A at § 6714.
118 Id.
promoting computer and Internet literacy taken during a high school student’s freshman or first year of secondary school. However, 34 CFR X(d) would contrast sharply with a general computer sciences or computer programming class. The objective of the 34 CFR X(d) is aimed at a more rudimentary introduction to computers and the Internet, as it would be impracticable to require every student to gain fluency in programming. The goal of 34 CFR X(d) is to provide a functional, working knowledge of computers and the Internet in a manner that prepares the student for safe, effective technology use in the future, irrespective of profession.

The following is a sample syllabus for 34 CFR X(d):

UNIT 1 – **Computer and Internet Set-Up**
- Computer, Monitor, Router, and Accessory Specifications
- Physical Set up of Computers, Monitors, Accessories
- Creating a Wireless Network

UNIT 2 – **Developing Fluency with OS Software**
- Introduction to Microsoft OS and programs
- Introduction to Macintosh OS and programs

UNIT 3 – **Introduction to the Internet**
- Theoretical Construction of the Internet: physical connections, routers, and major protocols
- Introduction to Web Browsers

UNIT 4 – **Introduction to Computer Security**
- Password Theory
- Firewalls and Anti-Phishing Measures

UNIT 5 – **Introduction to Computer and Internet Law**
- The Computer Fraud and Abuse Act
- The Internet Gang Prevention Act

**Examination:**
A pass/fail exam where a student must properly:
1. Set up a functioning computer

---

119 Ideally, this section would cover topics like RAM, processor speed, hard drive space, and other technical specifications to teach students how computers operate and why a specific computer may be better or worse for their needs.

120 Pass/fail here refers to a threshold level of competency on an exam needed to gain the “credit” needed for graduation: for example, if the threshold level is set at 70/100, and a student scores a 69, that student is ineligible for high school graduation.
2. Access and manipulate text, image, and video files on both Microsoft and Macintosh Operating Systems
3. Explain the framework of the Internet through multiple choice questions
4. Access specific websites or information on the Internet
5. Identify strong v. weak passwords
6. Determine which of a group of emails is a fraudulent phishing attempt and what specifically indicated the illegitimacy of the email
7. Identify which computer or online actions would violate federal law

This model curriculum need not be specifically followed by every public high school in the specific order listed, nor should only the topics proposed be taught. 34 CFR X(c) would be a straightforward, objective test that mimics the proposed examination in 34 CFR X(d). Timing is of the essence for 34 CFR X(c): giving the test to seniors or fourth year secondary school students solidifies the information learned in 34 CFR X(d) and guards against students solely learning a sufficient amount of information to pass 34 CFR X(d) that is thereafter forgotten.

34 CFR X(c) and 34 CFR X(d) would be effective deterrents to potential hacktivism in several ways. First, requiring 34 CFR X(d) as a freshman or first year class provides a safe, legal environment for students early on in their studies in a way that preempts a student from seeking out the same kinds of teaching from hackers or hacktivist groups. Second, 34 CFR X(c) provides a capstone that reinforces the information learned in 34 CFR X(d) at a key time before students leave for higher education with less parental or academic oversight.

3. The Need for a Solution

As a threshold matter, it is undisputed participating in any variety of a DDoS attack, as well as a whole host of other computer and Internet attacks, are
potentially punishable under the Computer Fraud and Abuse Act (CFAA).\textsuperscript{121} The indictment in \textit{Collins}\textsuperscript{122} alleged violations of the CFAA against various members of Anonymous for a DDoS attack involving the Low Orbit Ion Cannon against Paypal, Inc., in retaliation for Paypal’s limitations of donations to WikiLeaks.\textsuperscript{123}

As stated in Part 1, the increasing growth and popularity of Anonymous and other hacktivist organizations created two growing concerns: (1) the increasing politicization of Anonymous, which with increased membership, enthusiasm, and human capital has the potential to carry out even more cyber-attacks from a hacktivist platform, and (2) increased general attention to cyber-attacks, which prompts the threat of individual users acting as “copycats” acting individually and outside the scope of any organization.\textsuperscript{124} Any potential effective solution must acknowledge both threats.

This paper argues for a solution above and beyond the CFAA for three primary reasons: (1) the CFAA’s damage threshold limits its effectiveness, (2) the CFAA’s focus is on computer crimes and not the limitation of Internet gangs or hacktivist groups, and (3) the CFAA does not carry an educational component.

\textsuperscript{122} Indictment, at 2-6, United States of America v. Cooper, (No. CR11 00471 JF PSG), 2011 WL 2906181 (N.D. Cal.). This case is in its infancy, and the success of these allegations, while probable, are not known at the time of this paper’s completion.
\textsuperscript{123} See e.g., Xcentric Ventures, LLC v. Stanley, 2007 WL 1795811, at *1-4 (D. Ariz. 2007). Plaintiff, Xcentric, published a the website “Ripoff Reports,” a site that allowed users to report unethical or deceptive business practices. Defendant, Stanley, a member of the Defamation Action League, sent a variety of threatening letters to Xcentric on behalf of aggrieved businesses demanding that the site remove certain allegations by users. When Xcentric ignored the letters, Stanley launched a series of successful DDoS attacks against \texttt{www.ripoffreport.com}.\textsuperscript{124}
A threshold requirement for liability under the CFAA is a $5,000 damages component.\textsuperscript{125} This damages requirement has not been uniformly interpreted, and can act as a thorn in the side of courts and prosecutors. The United States District Court for the Eastern Division of Texas held that the $5,000 damages provision must be done to an individual computer, and cannot be spread across a series of computers.\textsuperscript{126} The Ninth Circuit held that the damages requirement can include the monetary investment needed to repair damage done by an attack to restore programs, systems and data\textsuperscript{127}; the Second Circuit, however, interpreted the CFAA in a completely different way, holding that travel costs associated with repairing the damage done by a computer attack did not factor into the CFAA damages threshold.\textsuperscript{128} Moreover, good will lost as the result of the attack was not a factor in calculating CFAA damages.\textsuperscript{129} Monetary damages should not be a bar to prosecuting hacktivists, especially when the damage done is predominantly political or ideological.

The purpose of this paper’s model statute is \textit{not} to criminalize a DDoS attack. Instead, a sample statutory purpose would read as follows:

\begin{quote}
The Internet Gang Prevention Act attempts to ameliorate the growing threat of cyber-crime perpetrated through hacking collectives known colloquially as ‘hacktivist groups’ by providing enhanced statutory penalties for criminal computer attacks done as a member of a hacktivist group. The Act further seeks to increase computer
\end{quote}

\begin{footnotes}
\item[127] United States v. Middleton, 231 F. Supp. 1207, 1213 (9th Cir. 2000). Here, the criminal defendant was convicted of illegally accessing e-mail accounts provided to employees at his erstwhile employer. The defendant subsequently deleted the e-mail accounts. He unsuccessfully argued at appear that the Trial Court misinterpreted the CFAA when instructing the jury that the damages component can include the “repair costs” of the damages.
\item[129] Id.
\end{footnotes}
and cyber literacy in the United States by providing penalties for schools failing to comply with 34 CFR X.

The model statute thus focuses on limiting the growing threat of Internet gang membership, while working in tandem with existing cyber-crime statutes that criminalize the actual attacks to ensure the first level of criminal liability.

The CFAA does not provide an educational remedy. While the threat of hacktivist groups targeting politically unaffiliated individual users is very low, the idea that the rise in hacktivism popularity will spawn increased numbers of copycats does pose potential threats to apolitical users. Increased public awareness and education is imperative in limiting (1) users from choosing to hack or join hacktivist groups and (2) maximizing the potential for the public at large to be aware of and possibly even defend against computer attacks.

Conclusion

It is clear, even to a layperson causally following the news and modern culture, that cyber-attacks are growing in popularity. Cyber culture will only continue to grow with technological innovation and increased interconnectivity. Legislators must act to limit the growth of hacktivism. The most effective solution to produce such a goal should entail two prongs: (1) a statutory intervention, which adds increased penalties for cyber-crimes committed as a member of an Internet gang or hacktivist group, and (2) an educational reform that has the dual effect of limiting individual users’ risk to cyber-crime through increased computer and cyber

---

130 See supra n. 106.
literacy, and encouraging computer learning in an environment that does not lead an individual to join an Internet gang.