Exploration of Potential Terroristic Radicalization of Hacktivist Collectives

A Dissertation Submitted To The Faculty Of The Henley-Putnam University Doctorate Program
In Partial Fulfillment Of The Requirements For The Doctor of Strategic Security

by
Harry Jackson
Herndon, VA
December, 2014
Exploration of Potential Terroristic Radicalization of Hacktivist Collectives
by
Harry Jackson
Herndon, VA
December, 2014

Approved:

____________________________________
Raymond J. Curts, PhD, Chair Date

____________________________________
Denise D. Greaves, PhD, Date

____________________________________
Donald L. Cummings, PhD, Date
Disclaimer

The views expressed in this clinical dissertation manuscript are those of the student and do not necessarily express the views of the Henley-Putnam University.
EXPLORATION OF POTENTIAL TERRORISTIC RADICALIZATION OF HACKTIVIST COLLECTIVES
Doctorate in Strategic Security

Permission is herewith granted to Henley-Putnam to make copies of the above title, at its discretion, upon the request of individuals or institutions and at their expense.

__________________________ Signature of Author

Extensive quotation or further reproduction of this material by persons or agencies other than Henley-Putnam University may not be made without the expressed permission of the author.
Abstract: The vulnerability of United States’ (U.S.) banking and critical infrastructure systems to cyberterrorist attacks has been the topic of several congressional debates (U.S. Congress, 2011). This study answers the question, “Are hacktivists radicalizing and are they likely to resort to acts of cyberterrorism?” Hacktivists are an offshoot of environment and animal rights groups such as the Earth Liberation Front (ELF) and the Animal Liberation Front (ALF), both of which have adopted the strategy of property destruction as a means to obtain their objective: to coerce corporations and government to end practices they despise by making those practices too costly to continue. The Federal Bureau of Investigation classifies the ELF and ALF as terrorist organizations (Jarboe, 2002). The results of the study indicate an increasing trend of hacktivist organizations primarily targeting government entities and that these groups are beginning to radicalize. It is likely that there will be hacktivist organizations that radicalize and resort to acts of cyberterrorism. To enable the posturing of government resources to prevent such acts and or mitigate their effects, there should be the development of an emerging warning problem to support the warning mission of the U.S. Intelligence Community.
# Table of Contents

Chapter 1: Introduction ........................................................................................................ 1  
  Problem Statement ........................................................................................................... 1  
  Research Question .......................................................................................................... 1  
  Purpose .................................................................................................................................. 3  
  Analysis and Results ......................................................................................................... 3  
  Summary .............................................................................................................................. 4  

Chapter 2: Literature Review ............................................................................................. 6  
  Transformation of Warfare and the Reality of Cyberterrorism ........................................... 8  
  Cyberterrorism .................................................................................................................... 17  
  Historical Culture of Hackers ............................................................................................ 18  
  Cyberspace as a Social Meeting Place .............................................................................. 20  
  Historical Links to Earlier Collective Activist Organizations: The Earth Liberation Front .... 22  
  The Advent of Hacktivism ................................................................................................. 28  
  Current Hacktivists Operational Attack Methods ........................................................... 32  
  Radicalization and Extremism ......................................................................................... 33  
  Possible Evolution of Hacktivists into Cyberterrorists .................................................... 45  
  Call to Action .................................................................................................................... 50  
  Combating Cyberterrorism ............................................................................................... 52  
  Summary .............................................................................................................................. 63  

Chapter 3: Research Methodology ..................................................................................... 64  
  Background ....................................................................................................................... 64  
  Research Design ............................................................................................................... 65  
  Sampling ............................................................................................................................. 66  
  Measuring Instruments ..................................................................................................... 66  
  Data Collection Procedures ............................................................................................. 67  
  Data Analysis ................................................................................................................... 68  
  Assumptions and Limitations ......................................................................................... 69  

Chapter 4: Data Analysis .................................................................................................... 71  
  Case Study Analysis: Evolution of Cyber Conflict ......................................................... 71  
  Hacktivist Trends ............................................................................................................. 80  
  Emerging Warning Problem ............................................................................................. 89  
  Environmental Scanning .................................................................................................. 90  
  Political Environmental Scans ....................................................................................... 92
The First Reported Indication of Radicalization of a Hacktivist Collective ................................ 100
  Social Environmental Scans .......................................................................................................... 104
Sort Out Which Scenarios to Explore ............................................................................................ 104
  Scenario 1—Baseline ..................................................................................................................... 104
  Scenario 2—Plausible .................................................................................................................... 104
  Scenario 3—Wildcard ................................................................................................................... 105
Chapter 5: Analysis and Conclusion ............................................................................................... 106
  Determine if There is a Warning Message in any of the Scenarios ............................................. 106
  Identify or Review ........................................................................................................................ 106
  Explore Opportunities .................................................................................................................. 108
  Recommendations ....................................................................................................................... 110
    Radicalization of Hacktivist Collectives Will Seek to Impede DOD Operations .................. 110
References ........................................................................................................................................ 116
Appendix A: Data on Hacktivist Collectives ................................................................................. 128
Appendix B: Social Scans ................................................................................................................ 148
Figures

Figure 1. Allied Organizations of the People’s Liberation Front. .......................................................... 26

Figure 2. Plausibility Limit. .................................................................................................................. 61

Figure 3. Number of Attacks From 1990–2013 .................................................................................. 83

Figure 4. Numerical Trends of Attacks From 1990–2013 .................................................................. 84

Figure 5. Hacktivist Acts, by Apparent Purpose ................................................................................ 85

Figure 6. Objectives and Motivations of Hacktivist Groups. .............................................................. 86

Figure 7. Trends of Hacktivist Attacks. .............................................................................................. 87

Figure 8. Anonymous YouTube Video Protesting CISA .................................................................. 96

Figure 9. Anonymous YouTube Video Protesting CISA .................................................................. 97

Figure 10. Anonymous YouTube Video Protesting CISA ................................................................. 98

Figure 11. Anonymous YouTube Video Protesting CISA ............................................................... 99

Figure 12. Protest Against Government Surveillance ....................................................................... 101

Figure 13. Protest of U.S. Federal Government Practices to Identify Terrorists ............................... 102

Figure 14. Promotion of Hacktivism ................................................................................................. 103

Figure 15. Trends of Hacktivist Attacks .......................................................................................... 112

Figure 16. Twitter Feed—Social Posts Informing Community Members of Potential Government Action When the Russian Government Attempted to Track TOR Users ........................................... 148

Figure 17. Twitter Feeds—Social, Posts Informing Community Members of Potential Government Action When Russia Attempted to Track TOR Users ................................................................. 149

Figure 18. Twitter Posts on July 30, 2014, Containing Critical Commentary and Protests of the Killing of Palestinians by Israelis in Gaza .......................................................................................................................... 150

Figure 19. Twitter Posts Containing Critical Commentary and Protests of the Killing of Palestinians by Israelis in Gaza .......................................................................................................................... 151
Figure 20. Twitter Posts Containing Critical Commentary and Protests of the Killing of Palestinians by Israelis in Gaza

Figure 21. Twitter Posts Containing Critical Commentary and Protests of the Killing of Palestinians by Israelis in Gaza

Figure 22. Twitter Posts Containing Critical Commentary and Protests of the Killing of Palestinians by Israelis in Gaza

Figure 23. Twitter Posts Containing Critical Commentary and Protests of the Killing of Palestinians by Israelis in Gaza

Figure 24. Facebook Posts Containing Critical Commentary on Israeli Actions in Gaza

Figure 25. Facebook Posts From July 30, 2014, Containing Critical Commentary on Israeli Actions in Gaza

Figure 26. Facebook Post From July 30, 2014, Containing Critical Commentary on Israeli Actions in Gaza

Figure 27. Facebook Posts From July 30, 2014, Containing Critical Commentary on Israeli Actions in Gaza

Figure 28. Facebook Posts From July 30, 2014, Containing Critical Commentary on Israeli Actions in Gaza

Figure 29. Cyber Intelligence Sharing and Protection Act (CISPA) Commentary From July 30, 2014

Figure 30. CISPA Commentary From July 30, 2014

Figure 31. Protest of Israeli Actions in Gaza Posted on Twitter Addresses the Killing of Anon Members

Figure 32. Commentary on Israeli/Palestinian Conflict Posted on 4Chan b Board

Figure 33. Commentary on Israeli/Palestinian Conflict Posted on 4Chan b Board

Figure 34. Promotion of the Hacker Values of Freedom of Information and Transparency of Government

Figure 35. August 7, 2014. Facebook Commentary Calling for Attacks on the NSA, IRS, EPA, and Other Government Agencies
Tables

Table 1. Research Questions to be Answered

Table 2. Code Collected Data Pertaining to Hacktivist Attacks

Table 3. Summary of Hacktivist Collectives Analyzed

Table 4. Environment Scanning Factors

Table 5. Answers to Research Questions

Table 6. Cult of the Dead Cow

Table 7. Syrian Electronic Army

Table 8. pHC, a Hacktivist Organization

Table 9. giest, a Hacktivist Organization

Table 10. ~EL8, a Hacktivist Organization

Table 11. Naija Cyber Hacktivists

Table 12. The People’s Liberation Front

Table 13. Cutting Sword of Justice

Table 14. Thehacker12

Table 15. Antisec

Table 16. Lulzsec

Table 17. Redhack

Table 18. Anonymous
Chapter 1: Introduction

Problem Statement

In 2007 and 2008, Estonia and Georgia, respectively, were the victims of cyber-attacks that crippled their communication and economic infrastructures in the midst of their respective disputes with Russia. These attacks are often referred to as the first instances of a new kind of warfare: “cyber war” (The Economist, 2008). It has long been acknowledged that the United States is also vulnerable to these kinds of cyberspace attacks. North Korea and China have conducted cyber-attacks against the United States several times in the past few years, and these strikes have been met with varying levels of successful responses. Terrorists recently have also been using the Internet to train and recruit personnel and coordinate attacks (Kaczynski, 2013). The bar of entry into cyber warfare, however, is low for state agents and terrorist organizations. From a resource perspective, a state or organization need only invest a few thousand dollars to develop its cyber capabilities (Lupovici, 2011).

Research Question

Are hacktivists radicalizing and are they likely to resort to acts of cyberterrorism? The Center for Strategic and International Studies (CSIS) has defined cyberterrorism as “the use of computer network tools to shut down critical national infrastructures or to coerce or intimidate a government or civilian population” (Tafoya, 2011). Table 1 contains the comprehensive list of research questions the study will answer. For the past 11 years, the United States has been conducting a war on terrorism, but thus far, the nation has never been the subject of a substantial cyberterrorist attack campaign by any particular group or individual—or at least not one that has
ever been acknowledged. The vulnerability of U.S. banking and critical infrastructure systems to cyberterrorist attacks has been the topic of several congressional debates (U.S. Congress, 2011).

The study will attempt to answer the question, “Are hacktivists radicalizing and are they likely to resort to acts of cyberterrorism?” Hacktivists are an offshoot of environment and animal rights groups such as the Earth Liberation Front (ELF) and the Animal Liberation Front (ALF), both of which have adopted the strategy of property destruction as a means to obtain their objective: to coerce corporations and government to end practices they despise by making those practices too costly to continue. Because the ELF and ALF engage in violent acts of property destruction, they are considered terrorist organizations by the Federal Bureau of Investigation (Jarboe, 2002). Hacktivist organizations, such as Anonymous, engage in the same activities that allowed extremist organizations such as the ELF and ALF to flourish: free speech and assembly.

The research study will examine the volatile talk of hacktivist collectives to ascertain the likelihood that it will transgress into cyber terrorist actions. Sub-topics will also explore the culture of the hacker/cracker community and the level of expertise required to become a hacker/cracker. Procedural questions will be posed using a phenomenological approach of inquiry to determine whether hacktivist organizations are at risk of radicalizing and becoming cyberterror organizations.

Phenomenological studies can assist in deconstructing and understanding terrorist campaigns and government responses (Yin, 1989). Terrorists often justify their tactics in the name of giving a voice to persons and groups that are underrepresented and suffer from perceived injustice (Global Focus, 2013). Terrorism is a means of communicating a message to a target audience. Many terrorists have used these means to communicate their messages, but they

1 A ‘cracker’ is known a malicious hacker, a person who conducts hacking as a part of a criminal enterprise.
have not yet done so on a large scale in cyberspace. Al-Qaeda terrorists have not conducted any cyber-attacks against U.S. interests; instead, they use the Internet solely to recruit members, conduct training, spread propaganda, and facilitate group communication.

**Purpose**

In many societies, hackers constitute a separate subculture. They tend to be highly independent and curious about the way things are and how they function, and they frequently attempt to modify devices and systems to allow them to perform unique functions (Strickland, 2013). Because they are so independent, many hackers have become “hacktivists,” persons who use cyberspace tactics and communication to promote political ends. The question of whether “hacktivism” can become “terrorism” will be considered an examination of the potential responses to cyberterrorism as a central theme of this study.

The United States has only recently begun to develop a doctrine for cyberspace operations against other state actors. Responses to attacks by organized non-state actors, however, have still not been doctrinally addressed. A plan for governmental responses to cyberterror attacks is also greatly needed because, to date, no publicly acknowledged government policies on the matter are available.

**Analysis and Results**

To explore the reasons why hacktivists have yet to resort to cyberterrorism and the likelihood that they will do so, the study will adopt a pragmatic approach by using a case study research and observation design. The study uses a collective case study design to analyze case studies about the terrorist-evolved use of information technology that ranges from chat rooms and message boards to virtual reality environments such as Second Life that could be used for training and rehearsal of attacks. Any of these platforms could also be used to coordinate
cyberterrorist activities. In this study, the researcher will also analyze cyber-attacks that have occurred over the past twenty-four years, including the attacks in Estonia and the distributed denial of service (DDoS) attack on American Express on March 28, 2013, which the so-called “cyber-fighters” of Izz ad-Din al-Qassam have claimed credit for, and the many attacks that have occurred since September 19, 2013, similar to the ones on Bank of America, JP Morgan Chase, Wells Fargo, U.S. Bank, and PNC Bank that raise concerns that hacktivists may resort to acts of cyberterrorism (Rothman, 2013; Soulskill, 2013).

Summary

The exact extent of the threat that cyberterrorism poses is debatable; however, there is some consensus that the formative stages of cyberterrorism are already being expressed within communities of “patriotic hackers” and “hacktivists.” Members of these groups are theoretical precursors to cyberterrorists just as many “patriots” and “activists” in the material, non-digital world have radicalized and become terrorists in the past.

The study will collect information from various entities to answer the question, “Are hacktivists radicalizing and becoming potential cyber terrorists?” The research will further explore the idea of cyberterrorism and the potential ways in which extant groups and actors could become cyberterrorists, and the research will identify opportunities to mitigate the threat. Table 1 contains a succinct list of the research questions addressed.
Table 1. Research Questions to be Answered.

**Research Questions to be Answered:**

1. Hacktivist motivations to conduct cyber-attacks.
2. Trends and patterns of hacktivist targets and attacks.
3. Possible online radicalization of hacktivists in a virtual environment.
4. Indicators of online radicalization.
5. The reasons why hacktivists have yet to resort to acts of cyber terrorism.
6. The likelihood that radicalized hacktivists will resort to acts of cyber terrorism.
7. Explore the value of developing an emerging warning regarding the potential threat of radicalized hacktivists conducting cyber terror attacks to further political agendas.

*Note. Source: author.*
Chapter 2: Literature Review

This chapter surveys the extant literature on the topics of the transformation of warfare, including cyber-warfare, the vulnerability of the United States to acts of cyberterrorism, the cultural history of hackers, the advent of hacktivism, and the likelihood of hacktivists morphing into cyberterrorists. The paper concludes with an analysis of works discussing various strategies that the United States could employ to counter this emerging threat.

Notable among the current literature on terrorist cyber-operations is Gabriel Weimann’s (2009) “When Fatwas Clash Online: Terrorist Debates on the Internet,” in which he discussed the ways that terrorists use the Internet to communicate, launch psychological campaigns, recruit new members, raise funds, promote violence, provide training, and plan and coordinate attacks. Weimann argued that terrorists are increasingly also using the Internet as a medium for debates and disputes and that, by examining these quarrels, counter-terrorism forces can identify the weaknesses in terrorist groups and exploit that information to combat them with divide-and-conquer strategies (Weimann, 2009).

Terrorist Internet forums could, indeed, provide a means of gauging which actions are accepted and supported within a terrorist’s constituency. In recommending them to state agencies as a source of actionable intelligence, however, Weimann failed to consider the three key characteristics of cyberspace that make it attractive to terrorists in the first place: anonymity, lack of attribution, and empowerment of the individual. Although a heated discussion on the Internet could potentially identify rifts within a terrorist organization, it could just as easily signify nothing. In such forums, it is difficult to determine whether people who are expressing disagreement or questioning the actions of a group are actually members in good standing of that
group, or if they are members of another organization or completely uninvolved individuals. Cyberspace grants everyone the opportunity to express their views anonymously. For terrorists, this is often a vital feature because they must often communicate clandestinely to avoid capture. The forums that Weimann analyzes may reveal the popular opinion within a terrorist community and may even include “official” statements from organizations to justify and rationalize their actions. Weimann does not, however, present adequate evidence to support his claims that these forums are an integral part of the decision-making process of terrorist groups and that the discussion and debate within them reveals accurate information about rifts within the organizations (Weimann, 2009).

In Economic Warfare: Risks and Responses, Kevin Freeman highlighted the vulnerability of the economic sector to cyber-attacks. He suggested the cause of the 2008 financial crisis was actually a deliberate financial attack and that the weak points in the global economic system that this strike exposed could be subject to further exploitation by entities intent on committing acts of financial terrorism. In his methodology, however, Freeman did not thoroughly examine the economic independence of global commerce. If he had, he would have addressed the possibility that Middle Eastern financiers of economic terrorism might, as rational actors, refrain from such attacks out of fear that the victims would discover their involvement and seek retribution that could cause harm to their own economic interests (Freeman, 2008).

In this study, this researcher addressed areas that Weimann, Freeman, and other scholars have neglected. Specifically, this researcher will explore the reasons why no terrorists have used devastating cyber-attacks against the United States even though the nation is in a time of acknowledged vulnerability. In addition, this researcher will assess the probability that one or
more of these groups will launch a cyber-attack before the United States has developed a robust defense to protect its critical infrastructures and industries from such cyber-attacks.

**Transformation of Warfare and the Reality of Cyberterrorism**

Cyberspace and its digital infrastructure were declared a “strategic national asset” by President Barack Obama in December 2009. In May 2010, the Pentagon established the new U.S. Cyber Command (CYBERCOM), which was tasked with protecting the military “.mil” domain and supporting the government “.gov” and commercial “.com” domains. Great Britain, China, Russia, and Israel are also organizing infrastructures for cyber-defense and the prevention of cyber-attacks and cyber-exploitations (Hsu & Marinucci, 2013).

A cyber-attack is an aggressive action meant to alter, disrupt, degrade, deceive, or destroy adversary computer systems, transmitting networks, or information in or generated from these systems and networks. Cyber-attacks can happen at a variety of ranges, from remote to close-access attacks. Examples of such attacks include but are not limited to viruses, supply chain attacks, operational compromises, and denial-of-service attacks. A cyber-attack has the potential to devastate the U.S. economy. Consider, for example, the effects of a successful denial-of-service attack on the computer systems used by any of the stock exchanges on Wall Street to envision what would happen to broader systems and society (Hsu & Marinucci, 2013).

Cyberspace is a new warfighting domain, or sphere for war, with a low barrier to entry, requiring only a few thousand dollars to acquire an operational capability. Because of this ease of entry, groups at all levels can engage in conflict in this domain; state actors, groups, and individuals are all active in cyberspace. *Cyber-war* is defined as an extension of policy through actions taken in cyberspace by state or non-state actors that constitute a threat to national security or occur in response to a perceived threat to national security (Shakarian, Shakarian, & Ruef,
2013). Nation-states, as opposed to individuals or groups, are currently in the lead with cyber-warfare capabilities. Highlighting the potential impact of cyber-attacks in *Cyber War*, Clarke and Knake (2010) claimed that the United States, Russia, and China are currently deploying cyberspace weapons to support their defense strategies in a manner similar to the way they used nuclear weapons during the Cold War. These nations are establishing military commands and “preparing the battlefield” or “shaping the battle space” by placing cyber-weapons, such as trapdoors and logic bombs, on key Internet sites. Paradoxically, even as the United States is preparing for an offensive cyber-war, it is pursuing policies that make it impossible to defend the nation from cyber-attacks (Clarke & Knake, 2010).

Clarke and Knake (2010) identified the inherent vulnerabilities in the structure, design, and use of the Internet in the United States. They paid particular attention to the level of federal dependence upon the Internet for both military and commercial applications, which could give adversaries who are less dependent on cyberspace a potential advantage in the event of a conflict. They also juxtaposed the extensive efforts by the Department of Defense to secure military networks with the current gaps in policy and law regarding the defense of networks in the civilian government and commercial sectors, even for critical infrastructure. Specifically, Clarke and Knake argued that the Federal Communications Commission (FCC) must use its regulatory powers to push Tier 1 Internet Service Providers (ISPs) to do more to protect cyberspace. Defense measures employed by ISPs might include disconnecting users from the Internet if they are known to be part of a botnet2, a collection of Internet-connected programs that communicate with other, similar, programs to perform tasks, while informing those users that their computers are infected and providing them with free antivirus software (Clarke & Knake, 2010).

---

2 A botnet is a network of computers communicating with one another to perform automated tasks.
Critical national infrastructures ranging from vital emergency communications channels to electrical grids are at risk of large-scale cyber-attacks. They have consequently drawn the attention of the U.S. federal government (United States Computer Emergency Readiness Team, 2014). According to a 2007 congressional committee report, the U.S. is “paying enormous costs for relying on such an insecure infrastructure” in terms of risk of a major disaster (Goodman & Lin, 2014, p. xi). The report drew attention to the “ominous” and constant threat created by the open environment by stating, “Cyberspace in general, and the Internet in particular, are notoriously vulnerable to a frightening and expanding range of accidents and attacks by a spectrum of hackers, criminals, terrorists, and state actors who have been empowered by unprecedented access to more people and organizations than has ever been the case with any infrastructure in history.” A dramatic rise in computer and Internet-related offenses since the 1990s reinforces the seriousness of the situation (Nhan, 2010, p. 3). As recent as June 2014, Eastern European based hackers successfully infiltrated the networks of power companies in France, Spain, and the U.S. and may already possess the capability to conduct cyber-sabotage attacks (Hesseldahl, 2014). It may be just a matter of time until we are attacked.

Michael Vatis (2006), a partner at Steptoe & Johnson and a former head of the FBI’s computer crime program, discussed how terrorists are already using the Internet and are actively exploring the U.S. information infrastructure, looking for weaknesses so that they can conduct a cyber-attack. Because of its relatively open borders, democratic liberties, and modern technology, the United States is vulnerable to foreign attack and cyber-attacks, and cyberterrorism is an emerging threat to U.S. national security. Cyber-threats are no longer limited to nuisances that only concern computer geeks. They have evolved to threaten the U.S. economy, the disruption of which would be serious and wide-ranging in its international ripple
effect. Denning (2001) and Vatis (2006) both asserted that, historically, terrorists have preferred attack methods that cause blood and gore (Denning, 2001; Vatis, 2006). However, terrorist organizations such as Al Qaeda have morphed into loose coalitions of like-minded groups and individuals worldwide that are willing to use any attacking methods within their means, including cyber-attacks. Vatis (2006), like Gable (2010), cited the increasing frequency of cyber-attacks in general and concluded that cyberterrorism is inevitable.

In 2011, 18 of the 24 major (Cabinet level) U.S. federal agencies reported deficiencies and inadequacies in their information security controls for financial reporting. Assessments of information security controls conducted by the Inspector General that same year revealed that most major agencies had weaknesses in most of their major information system controls. The Government Accountability Office (GAO) identified vulnerabilities in systems that monitor and control physical functions and sensitive processes supporting the nation’s critical infrastructures (Government Accountability Office, 2012).

Cyber-threats to U.S. infrastructure and other assets are a major concern for policymakers. Government services, corporate business processes, and individual professional and personal pursuits frequently rely upon Information and Communications Technologies (ICTs). Many ICT devices and other components are interdependent, meaning that the disruption of one component will affect others. A denial-of-service attack, the theft or manipulation of data, or damage to critical infrastructure through a cyber-based attack could have significant effects on national security, to say nothing of its disruption to daily life.

Although there have been no unclassified reports published regarding a terrorist-initiated cyber-attack on U.S. critical infrastructure, the vulnerability of those critical infrastructures via the Internet has been demonstrated. In 2009, the Department of Homeland Security (DHS)
conducted an experiment, known as the Aurora Project, that revealed some of the vulnerabilities in the nation’s control systems for managing power generators and grids. The experiment involved a computer-based attack on a power generator’s control system that caused operations to cease and the equipment to be destroyed (Fischer, Liu, Rollins, & Theohary, 2013).

According to the National Security Agency (NSA), cyber-attacks on American infrastructure companies increased 1700% from 2009 to 2011. Between December 2011 and June 2012, cyber-criminals targeted 23 gas pipeline companies and stole information that could be used to disrupt or damage networks, according to the Department of Homeland Security (DHS). Going a step further, in December 2012, two U.S. power plants were attacked with malware that reached critical networks. Many of these attacks were attempts at cyber-espionage or the disruption of services, but there is an increasing trend toward cyber-attacks designed to disable or destroy infrastructure. A future cyber-attack could lead to the physical destruction of assets such as a pipeline explosion, an extended disruption in electricity, or the shutdown of transportation systems (McCaul, 2013).

Clark and Knake (2010) attempted to raise public awareness of the fact that the world’s powers are following military doctrines in shaping the cyber-battlefield. They also cautioned that the potential early results of cyber-war could mirror the effects shown in the opening scenes of the reimagined version of the television series Battlestar Galactica, in which a hostile force so thoroughly disables the defenses of its opponents prior to attacking that the defenders are left completely helpless when the strike finally comes. Although not completely outside the realm of possibility, the connection between this work of science fiction and actual modern defenses is far-fetched and unsupported by the authors’ work. As in many other sections of their book, such
as chapters three, four, and eight, Clarke and Knake (2010) claimed to be simply raising public awareness, but the result smacks of fear-mongering.

There are works that dispute Clarke and Knake’s (2010) claims that the threat of cyberterrorism is dire. One such work is from Bruce Schneier, the author of *The Battle for Power on the Internet* (2013). Schneier hypothesized that there is an epic battle for power being waged in cyberspace, and although criminal and terrorist elements have had some successes, these will be short-lived. He based this theory on the idea that any successes in cyberspace by distributed criminal and terrorist elements have been the result of their ability to adapt rapidly and make use of new technologies. Later, however, these early advantages are dwarfed by larger institutions and organizations that have more amplifying power when they figure out how to make use of the new technology. As examples, he cited actions that have turned the Internet into a series of cyber-fiefdoms, including corporate use of cloud computing and government use of mass surveillance. Corporations establish clouds to control content and data completely to prevent piracy. Governments, meanwhile, use mass surveillance to establish cyber-sovereignty to consolidate power, using the same social media channels that activist groups use to organize protests to instead identify suspects for arrest. In addition, governments around the world are investing in censorship, cyber-weapon, and consolidated cyber-defense technologies to further increase their power. While the distributed elements are more nimble and able to make faster use of the new power enabled by technological advances, institutional powers, while slower to adapt, use that new power more effectively (Schneier, 2013).

However, there are also works that support the claims of Clarke and Knake (2010). Willis, a global insurance organization, surveyed available regulatory reports for disclosures regarding cyber-exposures by the company’s clients. It found that only 15 to 21 percent of the
top 500 companies and 15 percent of the second-tier companies surveyed cited a perceived exposure to cyberterrorism (Ross, 2014). One recent study found that firms running Supervisory Control and Data Acquisition (SCADA) systems took 331 days on average to implement patches (Brenner, 2011; Greenberg, 2010). This could be a result of the fact that automatically patching an industrial control system can be dangerous because it creates the risk of crashing or slowing the industrial control unless it is done at the right time with the right sort of expertise. Additionally, they cannot be updated easily or quickly under any circumstances. There is little perceived urgency to correct these flaws. Most owners of SCADA systems expect government intervention or insurance to compensate them in the event of a cyber-attack and thus do not invest heavily in cyber-security (Brenner, 2011).

The industries most concerned about possible exposure to cyber-threats are health care, telecommunications, and finance. Those industries, on the whole, reported that cyber-threats could seriously harm their business operations. Subsequently, those industries also feature the highest number of exposures disclosed (Willis, 2013). As Brenner stated, “Sami Saydhari of the nonprofit Professionals for Cyber Defense thinks it [hardening corporate network security] could be done for about $5 million with three-to-five year’s preparation. The chief requirement would be expertise, which for the time being is limited to a small number of intelligence services” (pp. 113–114).

Hackers have probed and continue to test the networks of various federal and state agencies, the armed forces, and the commercial industrial base of the armed forces. These actions have already caused damage and compromised sensitive and classified information. Cybersecurity threats will continue, and will likely grow, as the U.S. economy becomes more connected and as the Internet continues to become a critical part of both business and daily life.
Criminals are becoming increasingly sophisticated in their efforts to steal from consumers, industries, and businesses in the United States, and terrorists and foreign nations continue to use cyberspace as a means of attack against the national and economic security of the United States (112th Congress, 2014).

In 2011, the Manila Bulletin published an article that claimed cyberterrorism was no longer just the purview of science fiction writers and paranoid survivalists, but rather a reality with the potential to cause more devastation than either chemical or biological weapons. In contrast, the hacker publication 2600: The Hacker Quarterly published numerous letters and articles from subscribers and hackers that claim that the U.S. government has overestimated the capability of hackers to carry out such attacks (justanothersubscriber, 2014). There are also blog reports of failed efforts by hacktivists attempting to coordinate and conduct attacks against the U.S. government on the scale feared and touted by federal officials (Huang, 2013). Furthermore, there has yet to be a major cyberterrorist attack that has resulted in loss of life. Despite these tempering influences, Huang (2013) asserted that complacency would be ill-advised.

Most facets of modern life are now connected in some way to computers, and the infrastructure that supports most societies is thoroughly integrated with the technological revolution. Nations depend on computers to operate electrical and telecommunications grids; military networks; gas and oil storage; and emergency services, including ambulance, police, and firefighter dispatch. All of these sectors are vulnerable to cyberterrorism. The threat of cyberterrorism is real, and our present laws may be inadequate to address it (Manila Bulletin, 2011).

**Russian Conflicts with Estonia and Georgia.** From 2007 to 2009, cyber-attacks against Estonia and Georgia suspected to have originated in Russia demonstrated the effects that
offensive cyber-operations can have on an adversary. In Estonia, for the first time in history, the cyber-attacks nearly resulted in the complete shutdown of a nation’s government and key infrastructure. The targets of the attacks included the Estonian presidency and its parliament, almost all of the country’s government ministries, various political parties, three of the country’s six largest news organizations, two of its biggest banks, and assorted firms specializing in communications. During its conflict with Russia in the summer of 2008, Georgia suffered similar attacks, which preceded more conventional forms of warfare such as the incursion of Russian troops into Georgian territory. In July 2009, cyber-attacks probably launched from North Korea paralyzed government agencies and banking websites in South Korea and the United States. Recently, Google, the International Monetary Fund (IMF), and Sony sustained cyber-attacks that damaged their business reputations and caused significant financial damage. Cyberspace is currently a contested domain among nation-states, terrorist groups, organized crime groups, insiders, and hackers, granting anyone with access to the Internet the ability to wreak havoc (Kenyon, 2009; Traynor, 2010).

During the Estonia-Russia conflict, Estonia’s electronic infrastructure was attacked by almost one million computers simultaneously. Most of the machines used in the distributed denial of service attack were American computers hijacked by unknown elements inside Russia. The Russian government denied any involvement with the attacks and exhibited no interest in searching for the group of Russian hackers that had taken responsibility for the attack. The Estonian case was not the first major cyber-attack in the history of the Internet, but it was the most widely publicized, because it crippled an entire nation that is enormously dependent on network communications and offered empirical proof of malicious hacking beyond the instrument of espionage (Laasme, 2011).
In addition to its obvious uses in international conflicts such as those discussed above, cyber-war can also occur between governments and non-state actors and can be financed by states. Cyber-war is the deliberate use of information warfare by a state, employing weapons such as electromagnetic pulse waves, viruses, worms, and Trojan horses to target the electronic devices and networks of an enemy state (Laasme, 2011). Cyberspace offers actors anywhere with Internet access three advantages in a conflict: Actors can easily choose the scale of their attack, the proximity of their targets, and the precision of their attack plans. Cyberspace offers an attacking force five characteristics: reach, free fire at will, mass targets, easy stealth, and a near-instantaneous high-capacity payload (Demchak, 2011).

**Cyberterrorism**

Acts of terrorism are premeditated, designed to affect a political structure, targeted at civilians and civilian installations, and conducted by ad hoc groups. The current U.S. war on terrorism will likely result in cyber-attacks against U.S. assets launched by terrorist groups, nation-states that provide support for terrorists, and hackers who sympathize with the terrorists. Cyberterrorism consists of computer-based attacks against an adversary’s assets and occurs where cyberspace and terrorism converge (Prichard & MacDonald, 2004).

**The United States May Have Already Been the Victim of Cyberterrorism.** While experts continue to debate the seriousness of cyber-threats posed to corporate and national infrastructures, the United States may have already been the victim of cyberterrorism. In September 2012, the Bank of America, JPMorgan Chase, Citigroup, U.S. Bancorp, Wells Fargo, and PNC experienced massive denial-of-service attacks which clogged their websites with data requests and rendered them unusable. A hacker group calling itself the Izz ad-Din al-Qassam Cyber Fighters claimed responsibility for the attacks in retaliation for a video made by amateur
filmmakers in the United States that mocked the Prophet Mohammed. Izz ad-Din al-Qassam pledged to continue to attack American banking sites along with targets in other countries including France, Israel, and the United Kingdom until the video was no longer available online (Perlroth, 2012).

The group called on volunteers to visit two web addresses that could cause their computers immediately to start flooding targets including the New York Stock Exchange, NASDAQ, and Bank of America. Most researchers hold that the effects of the two websites alone would not have been sufficient to carry out an attack of such magnitude. It was likely instead that the group had assistance from a nation-state sponsor. Many of the botnets that attacked U.S. financial institutions at this time originated within Iran. Izz ad-Din al-Qassam denied any affiliation with the Iranian government, but the attacks’ level of sophistication was likely beyond the group’s capabilities. United States government officials believe that Iran was behind the cyber-attacks as a way to retaliate for economic sanctions and online attacks by the United States. The U.S. Intelligence Community holds that Izz ad-Din al-Qassam is a cover for Iran, although the government of Iran has denied responsibility for the attack (Perlroth, 2013).

Historical Culture of Hackers

Genosko (2007), Gable (2010), and Coleman (2012) synopsized the original hacker ethic, championing the free sharing of information. Hackers traditionally value freedom, access, and transparency of information. This is demonstrated by the distribution of free software within hacker communities and codified in the Debian Constitution and the Debian Social Contract (Coleman, 2012). Hackers are typically fairly liberal, with a strong sense of individuality; they are committed to rational thought and critical reflection and to developing a high level of skill in their chosen field, and they place a high value on free speech and civil liberties. They are wary
of corporations and the federal government (entities that seek to hide information) and are generally skeptical of these entities’ motives in safeguarding information to protect their competitive advantage and national security. Hackers assert a form of individualism and self-expression, and their society, as a whole, alternates between communal populism and individual elitism. Hackers proclaim that their ethical values are freedom, free speech, privacy, individual wit, cleverness, ingenuity, and meritocracy (Coleman, 2012).

**Technolibertarianism.** Paulina Borsook, noted in her social anthropology work that the high-tech culture is one of technolibertarianism, a tendency toward libertarianism and anti-regulatory/pro-market bias facilitated by technological innovation. Borsook described technolibertarianism as a political “way of being in the world” rather than any actual voting pattern (Borsook, 2000, p. 119). Due of their conceptual dismissal of government, technolibertarians typically do not engage in conventional political maneuvers and know little about driving institutional change. Borsook divides technolibertarians into four subgroups: ravers, gliders, catos, and cyberpunks. The fourth subgroup, cyberpunks, is the most germane to understanding hacker culture (Borsook, 2000).

The cyberpunk and sometimes criminal elements of high-tech culture—hackers and their malicious cousins, crackers—are simply more madcap manifestations of other, better-known individualistic and asocial qualities that are already present in technoculture. At their most extreme, cyberpunks exhibit some commonalities with the paranoia, self-importance, and displaced anger of militia members who are obsessed with privacy (Borsook, 2000).

The cyberpunk culture is one not often concerned with conventional notions of dress or grooming, whose members frequently keep nocturnal schedules or “vampire hours,” as they are sometimes called. It is also one whose members have workaholic tendencies, sometimes
dedicating even their recreational time to extended periods spent at the computer. In many cases, their activities walk the line between playful and criminal; favorite hobbies of cyberpunks often include breaking into computer networks and systems in an impish, playful, non-malicious, Kilroy-was-here way and tweaking federal government websites to demonstrate that they are not secure, but not doing any lasting harm in the process. These activities are classic computer hacking in its most time-honored, benign form (Borsook, 2000, p. 90).

While most hackers exercise their skills and interests in benign, if sometimes legally questionable ways, hacking in its destructive or malicious form is rightfully decried by many within the high-tech industry. Cyberpunks, for their part, see it as the antisocial mucking-up of the online sandbox. However, malicious hacking, which is properly termed cracking, can be perceived as simply a more extreme degree of the same activities performed by cyberpunk technoliberarians who hack playfully. In many ways, hacking can be interpreted as technolibertarianism gone feral; this is, in fact, how cyberpunkery is often characterized (Borsook, 2000).

**Cyberspace as a Social Meeting Place**

Michael Osit’s study, *Generation Text* (2008), asserted that today’s young generation has unprecedented access to information technology. Osit claimed that information technology has become a crutch for this generation that hinders their social development, as they are continually distracted and therefore have difficulty focusing and concentrating. According to Osit, today’s youth face constant interruptions in the form of instant messaging, email, Twitter, and other social media—a reality that denies them the luxury of focusing on one item or task at a time. This has negatively affected their social development, dampening their ability to control impulses through adolescence, and their ability to associate bad decisions with negative
consequences (Osit, 2008). In *Alone Together* (2013), Sherry Turkle described how individuals in modern society are relying on the virtual world for social interaction to the point of immersion, while social interaction in the real world suffers. With more people relying on cyberspace for their social interactions and community-building needs, it becomes simple to mobilize groups to take hacktivist actions. With poorer impulse control and a greater connection to the online world, today’s youth may be easily persuaded to join hacktivist or cyberterrorist causes without fully understanding the consequences of their actions.

In the past, social movements relied upon on direct interaction among physically present people to communicate their goals and ideologies, a strategy complemented by the use of media such as leaflets, brochures, and newsletters to reach large numbers of people both within and outside the movements. Technology has facilitated more rapid and thorough communication of social ideologies; newspapers, radio, and television cover major movement activities and communication by social movements is facilitated by telephones, copy machines, and fax machines. Social movements could not exist without sustained interactions both internally and with their external reference groups, pointing to the centrality of communication and to the attractiveness of using Internet Communication Technologies (ICTs) to distribute messages to a broad audience (Loader, Nixon, & Rucht, 2004).

Social media have expanded the reach of any given individual, and social networks have enabled individuals to share resources in an unprecedented manner. In previous generations, sharing information typically had to occur in person, although the advent of radio and television provided significant disintermediation. Today, being physically present is no longer necessary to interact or communicate efficiently; information technology makes it possible to share information very quickly over long distances. Activist groups are using the web to reach out to
other groups and form bonds and relationships that previously did not exist. They are also using the web and social media tools to organize spontaneously, resulting in events such as the 1999 protests at the World Trade Organizations (WTO) in Seattle (Bauerlein, 2011).

**Historical Links to Earlier Collective Activist Organizations: The Earth Liberation Front**

**The Earth Liberation Front.** Leslie James Pickering, a former spokesperson for the Earth Liberation Front (ELF) and self-acknowledged anarchist, has described the ELF’s common guidelines as follows:

1. To cause as much economic damage as possible to a given entity that is profiting off of the destruction of the natural environment and life for selfish greed and profit.
2. To educate the public on the atrocities committed against the environment and life.
3. To take all necessary precautions against harming life. (Pickering, 2007, p. i).

Pickering has argued that direct action taken by the ELF and similar organizations is part of a larger struggle for revolutionary change (Pickering, 2007).

The ELF is an international underground collective organization that uses direct action in the form of economic sabotage to coerce corporations and governments to stop practices the group deems reprehensible, by making the practices to costly. The organization lacks a general command structure; it is composed of small groups or cells that operate independently and anonymously, although they all profess the same ideology and share similar goals (Pickering, 2007).

The ELF’s self-described use of “economic damage” as a strategy has led to the group’s classification by the FBI as a domestic terrorist organization. In the film *If a Tree Falls: A Story of the Earth Liberation Front*, Marshall Curry and Sam Cullman (2011) explored the ramifications of the group being labeled a terrorist organization by the federal government. The
group’s activist strategies involved property destruction, which brought them to the government’s attention.

Consistent with the former FBI domestic terrorism section chief, James F. Jarboe’s work, members of ELF often display a deep suspicion and mistrust of the federal government (Public Broadcasting Service, 2011). Such mistrust often manifests itself in the form of conspiracy theories, such as the idea that the government is using the expanded powers granted to it by the PATRIOT Act to label groups such as ELF as terrorists, thereby gaining the authority to mercilessly persecute them to protect corporate and government interests (Curry & Cullman, 2011). Police actions to crack down on protest groups, such as the use of pepper spray, concussion grenades, and rubber bullets, have only further radicalized individuals involved in these protest actions (Curry & Cullman, 2011). Curry and Cullman’s film highlighted the widespread belief within the activist group that members cannot work within the system to accomplish their goals. Instead, ELF members believe that the system is designed to support the interests of the government, which, in turn, supports the interests of corporations and businesses (Curry & Cullman, 2011). As a result, the group believes that its actions are necessary to bring about social change by applying pressure to the government and corporations (Curry & Cullman, 2011).

These radical activists do not believe the government will take action if they restrict their protests to legal means. The thought prevails that the government does not consider them a voice to be heard, and many believe that whatever legal action they might pursue would be undermined. An example radical activists use as the power of their tactics was the arson of a Bureau of Land Management farm. This illegal act brought about within one day the closure of the farm—a result that mainstream activists were unable to accomplish over the course of 10
years of using legal methods, such as writing letters to government officials. Because the horse farm did not reopen after the arson, the members of ELF came to see such direct action as the most effective means of bringing about social change (Curry & Cullman, 2011).

The directors of the film took pains to capture the culture of the ELF, which does not view property destruction as an act of terrorism. When discussing the definition of what constitutes a terrorist, most organization members reply that they consider themselves freedom fighters. In contrast, they think that the actions of corporations and the government fit the definition of terrorism more closely, making those entities the actual terrorists (Curry & Cullman, 2011).

**Property Destruction as Violence.** Best and Nocella (2004) cited Ghandi and Dr. Martin Luther King, Jr. to support the position that property destruction is an act of violence. Ghandi stated that “Sabotage is a form of violence” (Best & Nocella, 2004, p. 233). Dr. Martin Luther King took a similar stance in March of 1968 when he led a march in Memphis on behalf of the city’s sanitation workers. When teenagers began breaking windows, King declared that he would never lead a violent march, called off the protest, and sped away in a nearby car (Best & Nocella, 2004).

Pickering initially claimed that the ELF is nonviolent, but later recanted in his resignation letter, acknowledging that the ELF’s actions are violent and defining violence as any act that aggressively harms or threatens to harm anyone or anything. However, he continued to support the actions taken by ELF members to further their cause, stating that he does not believe that nonviolence is the only legitimate means by which to struggle for liberation (Pickering, 2007).

**Links to Future Hacktivists.** The ELF has begun to share resources among members, including sharing training techniques, listing useful devices, and suggesting which methods and
techniques are most destructive or have the most significant effects. ELF members also practice cryptology in what they call the “book club,” in which ELF cells use the same book to encode and decrypt secret messages sent between the various cells. Several ELF members are computer scientists who have contributed computer hacking skills and tools such as Pretty Good Privacy (PGP) to encrypt data and messages to help facilitate the group’s activities. These technological efforts can be seen as the beginnings of hacktivism, linking activist groups such as the ELF with hacktivist groups such as the People’s Liberation Front (PLF) (Curry & Cullman, 2011).

**Relationship with the People’s Liberation Front.** The PLF formed in 1985 with a focus on the exploiting of Private Branch Exchange (PBX) telephone systems. The group has two operational divisions, one dedicated to covert operations, and the other to public campaigns. The mission of the covert operations division of the organization is to assist ‘freedom fighters’ and groups around the world by providing them technical assistance, intelligence gathering, electronic security, and cyber warfare capabilities. The mission of the public campaigns division is to maintain an open command structure that allows for the creation of temporary Internet ‘armies’ to launch DDoS attacks against what the group deems are ‘the enemies of freedom’ (Peoples Liberation Front, 2014).

Allied organizations with the PLF are:

1. “Chaos Computer Club
2. Anonymous Operations
3. Pirate Party International
4. Free Hackers Union of Syria
5. Crewl Underground Madness
6. Global Liberation Network
7. Internet Defense League
(Peoples Liberation Front, 2014)
8. Cult of the Dead Cow
9. Soldier X Group
10. Naija Cyber Hacktivists
11. Silver Liberation Army
12. RedHack
13. Animal Liberation Front
14. Earth Liberation Front”
Figure 1. Allied Organizations of the People’s Liberation Front. This figure illustrates the affiliation of the hacktivist organization with violent animal rights and environmental activist groups. Adapted from “Peoples Liberation Front,” http://plf.eu.pn.

**Further Radicalization of Members.** The documentary by Curry and Cullman detailed increasing radicalization among ELF members. One example described an incident in Washington in which the ELF incorrectly targeted a facility it thought was trying to produce genetically engineered trees. The information on which the ELF cell based its attack turned out to be faulty, and some members regretted the attack. In the wake of this action, the group began to splinter. Some members felt that the group did not go far enough. These members wanted to target individuals, specifically captains of industry (Curry & Cullman, 2011).
Ron Arnold, executive vice president of the Center for the Defense of Free Enterprise, has asked, “What happens when the next generation comes along and gets tired that these arsonists, these ecoterrorists, aren’t doing enough?” (Best & Nocella, 2004, p. 304). It is possible that activists, particularly if frustrated in their efforts, will become radicalized into terrorists.

**Relationship with Ted Kazcinski.** Ted Kazcinski, the Unabomber, admitted in court that he located his last two murder victims when their information was published in *Earth First!* Furthermore, in 2002, Kazcinski was listed on an ELF website (www.spiritoffreedom.org.uk/elf.htm) as a “Prisoner of War.” This same website also solicited financial donations from visitors to assist Kazcinski.

**Opportunities to Defeat Collectives.** A social activist group such as the ELF shares common attributes of its group membership with other social activist and hacktivist groups such as Anonymous and Lulzsec. For instance, members tend to come from all different walks of life. This diversity is a source of strength for the groups, though it can also be one of their weaknesses. Differences among members and their various personal backgrounds can be exploited to compromise the group and dismantle it. The ELF members responsible for the arson incidents in Oregon in the 1990s were brought to justice years later when one cell member, who had a drug problem, was eventually compromised by law enforcement; he subsequently became an informant and worked to bring the other members to justice (Curry & Cullman, 2011).

This same weakness existed in the Lulzsec organization. One of its core members, Sabo, was also compromised and convinced to become an informant. The information provided by Sabo was used by law enforcement authorities around the world to arrest members of Lulzsec and defeat the organization (Olsen, 2012).
The Advent of Hacktivism

Hacktivists are individuals who perform cyber-attacks for pleasure or for philosophical or other nonmonetary reasons; the activities of these groups can range from simple nuisances like denial-of-service attacks to disrupting government and private corporation business processes (Fischer et al., 2013). Hacktivist movements typically lack central leadership and are not bound together by any ism. They tend to be quite diverse, composed of widely scattered individuals connected mainly by the Internet and other information technologies (Boggs, 2012).

Historically, hackers themselves have not been politically active. Those political causes with which they have involved themselves have typically been confined within the narrow realm of pursuing software or information freedom (Coleman, 2012). Hacktivism is a relatively recent phenomenon that hackers have employed to protest perceived injustices against free speech, privacy, and the freedom of the individual. The growth of hacktivism is largely a result of the wide availability of the Internet and its significant presence in daily life. Furthermore, hacktivism offers several advantages over physical forms of protest and attack, such as global visibility, low cost, and a lack of geographical and distance constraints (Denning, 2001).

Denning (2001) asserted that hacktivists have little to fear from prosecution, as they are often able to operate anonymously. Though they have the knowledge, skills, and tools to attack computer systems, hacktivists generally lack the motivation to cause severe economic or social harm (Denning, 2001). For the most part, activists have turned to Internet tools to coordinate protests and disseminate messages to support their causes rather than to pursue malicious activities (Loader et al., 2004). The Anonymous group, the most famous hacktivist collective, fluidly backs a variety of activist causes, while most of its members support the group not by engineering cyber-attacks themselves but by contributing their computer power to provide
bandwidth to support a larger direct denial of service attack (Shakarian, Shakarian, & Ruef, 2013). Anonymous is a so-called “do-ocracy,” as the group rules by doing. Individuals propose actions that others may join; the Anonymous flag is then flown over the result to claim credit for successful attacks. There is no central authority to grant permission or to give praise or credit, so every action must be its own reward (Norton, 2012).

Jordan and Taylor (2004) analyzed hacktivists as the first social movement of the virtual realm (Jordan & Taylor, 2004). They stated that cyberspace is analogous to the Wild West and open to colonization in accordance with technolibertarian values of freedom of speech, freedom of information, and open access to all information. The movements of collectives such as Anonymous are compatible with the culture of citizen journalism, but with an aggressive, activist stance enabled by cyber-tools (O'Keefe, 2013). Both seek to enhance institutional transparency and expose wrongdoing, but by different means.

Olsen (2012) delved into the hacktivist culture of collectives such as Anonymous, LulzSec, and Antisec. She highlighted the hacktivist ethos of making information free and exposing corporate and government corruption. The advent of hacktivism has caught governments and corporations off-guard, exposing corruption and misconduct in various agencies and businesses. Hacktivist methods significantly shaped the Arab Spring in North Africa and the Middle East, exposing governmental practices to the international community and enlightening the citizens of the affected countries about their governments’ actions. Olsen (2012) discussed in depth the evolution of hacktivists from their roots as hackers trying to understand how their machines and networks worked to activists seeking to expose corruption within corporations and governments and to make information “free.”
Hacktivists hold the freedom of information in the same high regard as their hacker brethren and admire the work of Wikileaks owner Julian Assange and NSA whistleblower Edward Snowden. Assange, an Australian hacker, founded Wikileaks to support his hacktivist agenda, protect free speech, and expose power brokers to public scrutiny and transparency (Fowler, 2011). Assange’s site serves as a medium for disseminating sensitive corporate and government documents obtained from anonymous sources. Assange has often portrayed himself in interviews and media reports as an activist whose mission was to expose the truth for the greater good; he has implied that he wanted to start a revolution (S., B., (Producers), & Condon, 2013). Snowden, meanwhile, released documents that revealed NSA data-collection operations conducted on U.S. allies such as Germany and Brazil, as well as collection activities centering around American citizens. Snowden styled himself as a hacktivist who revealed sensitive U.S. intelligence information because he wanted to change U.S. policy. Elaborating on his motivations, Snowden proclaimed his desire for the American public to have a say in how they are governed. During his time in the employment of Booz Allen Hamilton as a contractor supporting the National Security Agency, Snowden came to believe that the NSA had become a dangerous machine of mass surveillance with unchecked power. He believed that the agency’s closed-door oversight by Congress and the Foreign Intelligence Surveillance Court was a “graveyard of judgment,” and that these entities were manipulated by the very agency they were supposed to keep in check. Snowden purported to be astonished to learn that the United States collected more information on American citizens than on rival nation-states, such as Russia, and believed that he needed to take action. He released sensitive documents and defected from the United States in order to alert the American public to the situation in the hopes that an outraged citizenry would begin to enact change (Washington Post, 2013).
Knappenberger (2013) further expanded on hacktivist culture, presenting hacktivist organizations as loose collectives of individuals who believe that truth wants to be free and that they are there to assist in the process (Knappenberger, 2012). However, Knappenberger identified many different facets to hacktivist culture. Hacktivist organizations such as Anonymous form from a series of virtual relationships, much like a kaleidoscope. They tend to form and disband in support of particular causes or to pursue causes with increased intensity, as in the cases of LulzSec, Antisec, Th3CabinCrw, and Malsec (Olsen, 2012; Knappenberger, 2013).

LulzSec, an offshoot of Anonymous, was the group responsible for a malicious attack on SonyPictures.com to point out that the company’s IT security was inadequate. The group has portrayed itself as a defender of human decency and civil rights, engaging in activities such as accusing Arizona law enforcement of racial profiling and corruption. The group only lasted 50 days before being intercepted and shut down by law enforcement. Another offshoot of Anonymous, Th3CabinCrw, launched “Operation Satiagraha” in response to the Brazilian government’s initiative to control Internet content available to its citizens. Under this initiative, the group posted captured confidential information. Members of Th3CabinCrw were arrested and the group disbanded after “Operation Pig Roast,” in which group members used Structured Query Language (SQL) injection to hack into the websites of U.S. police departments and other government-affiliated departments (Shakarian, Shakarian, & Ruef, 2013).

Malicious Security (Malsec) formed after the disbanding of LulzSec. Its members were mostly former Anons (members of Anonymous) who claimed to refocus their efforts on political activism. The group asserted that it would avoid harming individuals during its pursuit of social critiques and activism. Malsec began its activities through extensive use of blogs and social
media such as Twitter and Facebook. Later, the group would expand to more active engagement, tampering with assorted websites. It evolved its target selection to include government and government-affiliated sites as well as corporate banking websites in Romania, Bhutan, and the Philippines. In March 2012, Malsec compromised the website of Security Centre Ltd. on the Cayman Islands, defacing it and leaving behind a to-do list on how to fix the security issues that allowed the hack (Shakarian, Shakarian, & Ruef, 2013).

**Current Hacktivists Operational Attack Methods**

**Categories of Attacks.** From 2010 to the middle of 2011, hacktivist attacks fell into one of two categories, Reactive and Proactive. Reactive attacks are those stemming from an incident that inspires hacktivist collectives to attack a target. Such incidents include the attacks on MasterCard and Visa when the two credit card companies made the decision to deny the processing of payments and/or donations to WikiLeaks. Proactive attacks were those attacks a hacktivist collective announced before they assaulted its target. Anonymous’ threat against Mexican drug lords are an example of a proactive attack, though, the attack itself never materialized (Imperva, 2012).

**Types of Members.** Hacktivists typically employ the same hacking methods that profiteering hackers use and will often try to steal data first before resorting to more brute force measures such as a DDoS attack. There are two types of members within a hacktivist collective: skilled hackers and laypeople. The skilled hacker group is the most dangerous. They are capable of writing their own code and tools and display genuine hacking skills. Typically, a hacktivist collective has no more than 10 to 15 individuals who are skilled hackers. The second group, laypeople (also known as “script kiddies”), are individuals with few skills who can use
automated hacking tools with little to no training. The number of people in this group can be quite large, ranging from anywhere from a few dozen, to a few hundred (Imperva, 2012).

**Phases of a Hacktivist Operation.** Hacking operations fall into three phases:

1. **Phase 1: Recruiting and communications phase.** In this phase, hacktivists frequently leverage social media to recruit members, promote their campaign, and justify attacking the targets selected.

2. **Phase 2: Reconnaissance and application attack phase.** In the second phase, hacktivists will attempt to mask their identity and base of operations as they probe target applications to identify weaknesses that could result in a data breach.

3. **Phase 3: DDoS phase.** If a data breach fails, the skilled hackers group will often elicit help from laypeople, who, in large numbers, will download attack software to conduct more destructive actions, such as a DDoS attack.

**Differences Between Hacktivists and Profiteering Hackers.** There are some key differences between hacktivists and profiteering hackers. Though they do develop some custom built applications, they typically rely on inexpensive, off-the-shelf tools to conduct attacks. They also tend not to use botnets or rely upon malware as profiteering hackers nor do they often develop phishing or spear phishing emails. Lastly, a key difference between hacktivists and profiteering hackers is their method of recruitment. Profiteering hackers tend to recruit members in private hacker forums, whereas, hacktivists recruit openly in social media outlets (Imperva, 2012).

**Radicalization and Extremism**

McCauley, Moskalenko, and Sunstein discussed the phenomenon of group radicalization. McCauley and Moskalenko identified 12 separate mechanisms of political radicalization that can
move individuals, groups, and the masses toward increased sympathy and support for political violence. In their analysis, McCauley and Moskalenko relied on case studies on Russia in the 1800s, the United States in the 1970s, and on radical Islam after the fall of the Soviet Union at the end of the Cold War in the 1990s. Their analysis and synthesis of the case studies resulted in their conclusion that terrorism is an extreme form of radicalization; its pathways are described in their proposed 12 mechanisms that lead to exceptional violence in conflicts between state and non-state actors (McCauley & Moskalenko, 2011).

McCauley and Moskalenko (2011) asserted that it is an oversimplification to describe terrorists as individuals who are either evil or crazy and who conduct complex acts of violence to further political ends. Their analysis rings particularly true when examining the characteristics of members of such groups as the Weather Underground in the United States in the 1970s and The People’s Will in Czarist Russia in the 1870s, which shared almost identical traits. Both groups started out as organizations that conducted protests, eventually progressing to the use of violence. As McCauley and Moskalenko stated:

Radicalization is the development of beliefs, feelings, and actions in support of any group or cause in a conflict. Radicalization in response to threat is so reliable that terrorists can count on it as a strategy. Radicalization is not something that happens only to others—the mentally ill person or the evil character. It is a psychological trajectory that, given the right circumstances, can happen to any person, group, or nation. The trajectory is not right or wrong: it is amoral in the sense that radicalization can occur for causes both good and bad. (p. 4)

In their analysis of the members of the Weather Underground and The People’s Will, McCauley and Moskalenko stated that it would not be reasonable to assume that all members of terrorist
organizations are either evil or crazy. Rather, they are individuals committed to a cause and exclude the viewpoints of others.

**Individual Radicalization.** Western culture and psychology often interpret behavior as a reflection of the beliefs, feelings, and preferences of the individual. McCauley and Moskalenko (2011) identified six mechanisms of radicalization that are consistent with the Western default of individual attribution: personal grievance, group grievance, slippery slope, thrill-seeking, love, and unfreezing.

**Personal Grievance.** As it relates to the possibility of cyberterrorism and the radicalization of the individual who would be motivated to conduct such acts, the mechanism of personal grievance is the most applicable to the study of cyber-warfare. Suicide terrorism is a frequent result of the process of radicalization of individuals who have experienced a personal grievance. Groups such as the Chechen “Black Widows” often fit this description, as many of these women are seeking revenge against Russians for their own experiences of rape or for the deaths of husbands, brothers, or sons at the hands of Russian forces. The Tamil Tigers have also leveraged personal grievances to assist in radicalizing individuals in their groups of “Black Tigers,” which are typically composed of survivors of Sinhalese atrocities. There are also several accounts of Palestinian suicide bombers who cite attacks by Israeli Defense Forces against their neighbors or loved ones as the source of their personal grievances and their motivation to conduct suicide attacks (McCauley & Moskalenko, 2011).

Radicalization by personal grievance is fairly common, as it fits the familiar pattern of vengeful individuals seeking justice or retribution for a perceived wrong. The emotion underlying retribution and revenge is anger. There are two popular theories of anger; the first, originating with Aristotle, states that the perception of slight or insult leads to anger and becomes
a motivation for revenge. In this theory, insult evokes anger and a desire to retaliate.

Alternatively, pain-aggression theory contends that any punishing experience leads to anger and an increased propensity for aggression. Punishing experiences include not just frustration (being blocked from a desired goal), but any kind of discomfort. For example, animals shocked by electricity will try to bite anything in reach. This theory can be extended to people made to experience pain or frustration who may show increased and indiscriminate aggression. Pain-aggression theory is reflexive and less specific about the target of the resulting aggression: punishment makes the individual irritable (McCauley & Moskalenko, 2011). Denning (2001), Corley (2013; 2014a), and Kaye (2001) have frequently cited a sense of paranoia and the perception of extralegal persecution of hackers by the government. The atmosphere of anger against the government for persecuting hackers could potentially create a process of radicalization via personal grievance of an individual hacker (Corley, 2014; Corley, 2013; Denning, 2001; Kaye, 2001; McCauley & Moskalenko, 2011).

Individual radicalization leading to political violence is not common. It usually occurs as a result of a combination of personal and group grievances. In this blending of grievances, personal grievance equates to hostility toward a group seen as perpetrators of injustice, and group grievance equates to positive identification with a group seen as the victims of this injustice. These reciprocal positive and negative identifications provide stable incentives for intergroup conflict (McCauley & Moskalenko, 2011).

Slippery Slope. Minor involvements in political conflict can create forces that move an individual toward radicalization. An explanation for this phenomenon is rationalization. According to dissonance theory, humans are likely to change their opinions to fit their behavior, especially in circumstances in which they have committed a stupid or foolish act. They
subsequently come up with reasons that will justify or excuse their actions. As McCauley and Moskalenko (2011) stated, “Terrorist groups count on the power of the slippery slope in bringing new members to violence gradually. Testing recruits for obedience, testing to find undercover government agents, and desensitization to violence” (p. 44). After joining an underground group, new members are often required to participate in increasingly demanding activities. They usually begin their careers in the underground by distributing leaflets or renting an apartment for the group. The longer they remain with the group, the more likely they are to end up participating in robberies, assassinations, and other terrorist acts (Porta, 2006).

The power of the slippery slope is that it can move individuals to opinions and actions that they do not anticipate at the outset of their participation. There are terrorists who, looking back, cannot point out a particular moment during which they decided to become a terrorist; instead, “one thing led to another” such that it seems, in retrospect, inevitable that they would become terrorists (McCauley & Moskalenko, 2011).

Love, Risk-Taking and Status, and Unfreezing. The mechanism of love relates to loving an already radicalized individual, which can move another individual toward radicalization out of a sense of loyalty or solidarity. Risk taking and status concerns can also move individuals to radical political action. The group that is most susceptible to this phenomenon consists of young men who come from disadvantaged family backgrounds, have lower IQs, are of lower socioeconomic status, and who therefore have less opportunity in society along a traditional career path. Young men who fall into this category are more likely to be involved in gang activity, violent crime, drugs, and other high-risk behavior. Unfreezing occurs when previous commitments and attachments, such as family and or a career, that would bar a path to radicalization, are removed (McCauley & Moskalenko, 2011).
Group Radicalization. Three mechanisms can lead to group radicalization: group polarization, group competition, and group isolation. Group grievances frequently occur in response to political events or trends. As McCauley and Moskalenko (2011) stated, “The motivating grievance can be that of another individual or cause, even though this victimization does not include any direct harm to the one radicalized” (p. 24). This phenomenon is directly applicable to most causes pursued by hacktivist organizations. The capacity for positive identification extends beyond those near to and similar to the individual. During the process of group radicalization, the individual initially cares more about the welfare of groups that they are not a part of (e.g., Tibetans) or about the actions or welfare of individuals or groups that they do not know personally (e.g., a celebrity or a football team). In each of these cases, the individual’s concern for the welfare of the other goes beyond any immediate or tangible value to the self, and when that concern is threatened, conflict is likely to ensue (McCauley & Moskalenko, 2011).

Some groups are aggregations in which members share a sense of perceived interdependence, where what happens to one member of the group affects all members. Large aggregations can also share a sense of boundary and interdependence, becoming psychological groups (McCauley & Moskalenko, 2011). Sunstein has complemented the theories of McCauley and Moskalenko, stating that people can move toward violence as a result of their self-segregation. Sunstein (2009) asserted that political extremism, which often results in terrorism, is frequently a product of group polarization and that self-segregation is a useful tool for producing polarization.

An individual’s opinions in such settings are more likely to become increasingly extreme because their initial views have been corroborated by the assertions of the group and because they have become more confident after learning of the shared views of others. Social networks
can operate as polarization machines because they help to confirm and amplify people’s antecedent views (Sunstein, 2009). It is not hard to imagine this occurring in the hacker community in instances when community members rally to support another member facing criminal prosecution.

McCauley and Moskalenko (2011) have discussed two theories of group extremism resulting from group polarization to explain the phenomenon where discussion among like-minded individuals generates momentum that moves an entire group further toward extremism: relevant arguments theory and social comparison. According to the relevant arguments theory, a culturally determined pool of arguments favors one side of the issue over the other side. With social comparison, the theory is that the opinions of certain members within a group have social values attached to them. In this scenario, the direction (i.e., becoming more or less extreme) favored by the majority of group members before discussions begin is considered to be the preferred viewpoint. The individuals who favor that initial viewpoint are seen as more devoted to the group, and their extra status gives them more influence during group discussion. Furthermore, their views change less during the discussion.

In contrast, individuals who are less extreme or favor the majority opinion less have less influence and they change more during the debate. In an environment where no one wants to be seen as not supportive enough of the group-favored opinion, the result is that the average opinion becomes more extreme in the group-favored direction (McCauley & Moskalenko, 2011).

Sunstein (2009) again complemented the work of McCauley and Moskalenko by citing empirical findings suggesting that group members, particularly those of lower status, are hesitant to emphasize information that other group members lack. These lower-status members will often quickly suppress uniquely held information because of the difficulty of establishing its relevance.
and credibility and because of the risk of the group’s disapproval if they press a line of argument that others may reject.

Deliberating groups often move to extremes because they fail to elicit information that could steer them in a different direction. In many deliberating groups, people who emphasize uniquely held information are taking a social risk, of which they are often aware. In this dynamic, group members often underestimate the performance of low-status members and overestimate the performance of high-status members in a manner that gives high-status members a sense of deference that is not warranted by reality. This is a form of social cascading. As Sunstein (2009) stated, “When beliefs and perspectives spread from some people to others, to the point where many people are relying, not on what they actually know, but what (they think) other people think” (p. 90). The beliefs of individuals may be in error because they are relying not on their own private information, but on the proselytizing of other (high-status) group members, whom they trust. When people find themselves in groups of like-minded individuals, they are particularly susceptible to moving to extremes. The phenomenon of group polarization is a pattern typical of deliberating groups. It is not limited to specific periods, nations, or cultures and offers insight into the behavior of not only activists and terrorists, but also consumers, interest groups, and executive agencies (Sunstein, 2009).

Polarization typically has two functions: to reveal hidden beliefs and desires and to create new beliefs and desires. Group members frequently have a suppressed but deep-seated set of concerns that do not often materialize in their social life. These desires and concerns usually remain unspoken, but are frequently thought. In extreme cases, however, they are “unthinkable” in the sense that individuals cannot voice them in public without facing a serious risk of social disapproval, ostracism, or persecution. When group members speak with one another, those
suppressed concerns can come to the surface, and as group members exchange tales and reactions, the unthinkable comes out into the open. Extremism can result from this sharing, as group members feel outrage about practices that used to produce self-silencing mechanisms, revealing hidden beliefs and desires (Sunstein, 2009).

Group polarization frequently occurs because individuals fail to adjust their reactions to the skewed dynamics in which they find themselves and become susceptible to two types of group polarization: planned and spontaneous. Planned group polarization frequently involves polarization entrepreneurs who attempt to create communities of like-minded individuals, aware that these communities will not only solidify their positions, but move them in a more extreme direction. Spontaneous polarization occurs as a result of the voluntary participation of a group’s members without any planning or machinations (Sunstein, 2009).

Group polarization can occur even if there is no sense of grievance or if the suppression of hidden desires or beliefs has not occurred. In these cases, group polarization creates new beliefs and desires where “social influencers, involving the efforts of ‘polarization entrepreneurs,’ give rise to intensifying objections and growing protest. For many group members, the views that end up being extreme are entirely generated by group interactions. As they speak with one another, their inclinations to accept those beliefs are intensified. Here deliberation creates, for some or many, a series of objections that had previously been absent” (Sunstein, 2009, p. 32).

Group competition theory holds that groups define themselves in comparison with other groups. Cohesion emerges when group members feel that they share the same goals and values; working toward a shared goal cements loyalties, and the most reliable source of cohesion is intergroup competition. According to this theory, groups radicalize as a result of their
competition with other groups. Competition produces hostility toward the threatening competitor. The bigger the threat, the greater the hostility, which can create a slippery slope of conflict that ends in the perception of a zero-sum game that the group cannot escape. The group competition theory might apply to the radicalization of a hacktivist group if it perceives a threat from a government or corporate entity that moves the group toward unity of thought and action as its members prepare to combat that perceived threat (McCauley & Moskalenko, 2011).

Political competition can also result in radicalization when groups are in competition for the same base of sympathizers and supporters. As these groups compete for the same base, they might try different tactics to win support, escalating toward radical acts in an effort to “outbid” the other groups (McCauley & Moskalenko, 2011). For example, the activity of LulzSec may be seen as a form of political competition within the hacktivist community, with its attacks providing a way for the group to differentiate itself from Anonymous and attempt to gain mass support.

When a group’s lines of communication with other groups are severed, the power of group dynamics can result in radicalization through group isolation. Isolated groups tend to become all-important to their members. The extent to which these groups can become totalistic has a direct correlation with the extent of group radicalization. In isolated groups, members have unchecked power to determine value and meaning for the group. This acts as a force multiplier. Consensus power in such environments can justify extreme ideologies and lead to a conversion of group members akin to brainwashing; any threat to the group may be met with extreme action. In such groups, anyone and anything that matters exists within the group, and nothing outside the group is relevant (McCauley & Moskalenko, 2011). Over time, group polarization can be solidified as moderate members leave the group because they disagree with its direction. As
group members strongly consider resorting to acts of violence, a culture of voluntary sorting and self-selection appears in which “only the true believers remain,” who regard themselves as best friends or a surrogate family. This creates a dangerous condition for the group, as it is now composed of extremists, unified by bonds of affection and solidarity, and prone to discussions only among group members (Sunstein, 2009).

When a group experiences an exodus of members, it is prone to becoming more extreme, as the group will end up smaller and composed of more like-minded individuals who are more willing to take extreme measures. Internal discussions in such groups will likely produce more extremism. A group is also more likely to show extremist tendencies if it makes it easy for people to leave. If only loyalists stay, the group’s median member will likely be extreme and, likewise, internal discussion will produce increasingly extreme results. Once polarization or social cascading occurs and the group’s median view begins to move in a certain direction, any doubters and “halfway believers” will leave the group, while intense believers will remain. Although the size of the group may shrink, it may also receive new members who are even more committed, and the remaining members will, by self-selection, display more fanaticism. Group members may engage in self-segregation, either in a physical or informational sense, to protect their beliefs from challenge by outsiders and, as a result, group polarization will intensify (Sunstein, 2009).

Sunstein (2009) theorized that an effective way to create an extremist group or cult of any kind is to separate members, either physically or psychologically, from the rest of society. This separation can create suspicions about non-members and result in increased group cohesion. With such a separation in place, the information and views of outsiders can be discredited and
the process of group polarization can continue undisturbed as group members continue their internal dialogue.

When people engage in dialogue with only like-minded individuals, they have a tendency to amplify their pre-existing views and do so in a way that reduces their internal diversity. This phenomenon occurs in families, businesses, religious institutions, and other groups, including terrorist organizations. When members of a group perceive that they have a shared identity and high degree of solidarity, heightened polarization can occur, as calling to attention to group membership makes people far less likely to shift their views in those directions urged by people from different groups. As Sunstein explained, “If people are told that they are defined by their membership in a certain group, they will be less likely to listen carefully to those who are defined in different terms” (p. 43–44). Terrorists are made, not born, and deliberating enclaves of like-minded people often create intense phenomena of groupthink. Such groups become breeding grounds for extremist movements, situations in which terrorists leverage group polarization to move otherwise ordinary people toward committing acts of violence (Sunstein, 2009).

**Mass Radicalization.** Jujitsu politics, hatred, and martyrdom are the three mechanisms that contribute to the radicalization of mass populaces. Jujitsu politics is a strategy in which a terrorist group counts on an overreaction by a government to advance its cause and garner additional support. With jujitsu politics, it is essential to have distance or a “wall” between the government and the populace, making it easier for groups seeking to alienate the populace from its government. This creates an atmosphere conducive to the terrorist group, “a friendly sea to swim in.” The strategy of hatred comes into play in protracted conflicts where the adversary is dehumanized, encouraging the masses to view members of adversary groups as evil. In such a
scenario, it is possible to incite group members to attack perceived adversaries without regard to age, gender, or status. The final strategy, martyrdom, is one where a group constructs a martyr it can use to radicalize sympathizers to the martyr’s cause (McCauley & Moskalenko, 2011).

Laurie Willis (2011), in “Extremism: Opposing Viewpoints,” asserted that the most dangerous aspect of extremists is not that they are extreme, but that they are intolerant: “The evil is not what they say about their cause, but what they say about their opponents” (p. 14). According to Willis, individuals behave as extremists when they hold their own opinion as the exclusive point of view and do not allow for the possibility of different points of view. The views of the extremist often result in violence against those who do not share the same beliefs.

Willis (2011) tied her opinion of extremists to the motivations of terrorists, stating that they are motivated to act not by a sense of socioeconomic disadvantage, but by a sense of moral disgust. This disgust emanates from the terrorists’ point of view and the moral framework that they seek to impose upon others, along with their unwillingness to compromise or to consider alternative viewpoints. Willis concluded that the only way to defeat terrorism over the long term is to reduce the motivation for young people to radicalize in the first place.

Possible Evolution of Hacktivists into Cyberterrorists

Hacktivist groups such as Anonymous are not restricted to the English-speaking world. In April 2012, the media outlet #FreeAnons published a video declaring Anonymous’ support for a Turkish left-wing hacker group, R3dH4ck (RedHack). Members of this group compromised the computer network of the Turkish police and disseminated sensitive information to the public to expose the police as corrupt. Turkish authorities would later arrest seven people who appeared unrelated to the hacker group and declared R3dH4ck a terrorist organization. Anonymous retaliated, launching “OpSupportRedHack” in July 2012 and taking down the
websites of the Turkish Police Directorate (www.egm.gov.tr) and subpages of the Turkish National Intelligence Agency (www.mit.gov.tr) (Shakarian, Shakarian, & Ruef, 2013).

During the 2008 Georgia-Russia conflict, one phase of the operation shifted to the recruitment of “patriotic” Russian computer users who often referred to themselves as hacktivists. Many were thought to be members of the Russian youth movement, specifically the Nashi. Recruitment was primarily conducted through various websites such as StopGeorgia.ru that also posted cyber-weapons that users could download, paired with simple instructions and a list of target sites to attack. An interesting aspect of the Russian hacktivist attacks on Georgia, and a reason why the U.S. Intelligence Community believes Russia sponsored the attacks, was the professionalism of the site administrators. The site administrators supporting the malicious sites provided timely customer support to novice hackers, expelled unauthorized users of the site, and blocked traffic from U.S. IP addresses (Shakarian, Shakarian, & Ruef, 2013).

In *The Evolution of Cyber Terrorism*, Engelberg (2012) argued that the United States is a target-rich environment for adversaries seeking to leverage cyber-warfare to negate the conventional superiority the United States maintains in other areas (Engelberg, 2012). Criminals have already exposed vulnerabilities in cyberspace that terrorists could also exploit. The terrorist groups Hamas and Hezbollah have made use of cyber-attacks to augment their information operations to influence world opinion in their favor. Hezbollah uses the Internet to spread propaganda in a strategy it calls “cybercortical” warfare, a strategy of spreading propaganda aimed at Palestinian and Israeli audiences to portray Hezbollah not as terrorists, but as freedom fighters (Shakarian, Shakarian, & Ruef, 2013). To illustrate the extent of the threat that cyberterrorism poses, Engelberg (2012) used case studies of cyber-attacks that were conducted on U.S. corporations, such as Google, from IP addresses that originated in China.
Enghelberg (2012) also presented examples of attack vectors, such as spear-phishing emails, that hackers use in their assaults. She drew parallels between the political rhetoric of several terrorist organizations and communications from hacktivists to demonstrate that, although no attacks have yet occurred from that quarter, the potential for hacktivism to adopt cyberterroristic tactics and modes does exist.

**Viewing the Government as Persecuting Hackers.** Prominent in the hacker community is Eric Corley, editor of *2600 Magazine: The Hacker Quarterly*, that has been in print for the past 31 years. The publication serves as a social forum to share and distribute knowledge that subscribers can use to assist in maintaining anonymity online; protecting their privacy; learning how to manipulate devices and software to perform functions beyond their intended purpose; and, in some cases, learning how to commit crimes. The magazine also serves as a platform for awareness activism against government and corporate surveillance, suppression of free speech, net neutrality, and persecution of hackers in the community.

Since April 2013, the *2600 Magazine* editorial staff has taken a more activist stance against government surveillance. This was brought about by the disclosures of NSA data collection activities and programs by Edward Snowden. In April 2014, the magazine staff produced a scathing editorial on NSA activities claiming that the government has a history of overestimating hacker capabilities and that government data collection activities are for a more insidious purpose than combating terrorism. The staff claimed that government authorities have been attempting to collect personal information on the citizenry for more than 30 years, implying that the events of September 11, 2001 served as an excuse to execute agendas to collect this information in the name of national security (Corley, 2014b). The staff frequently claims that the government has a tendency to overestimate the capability of hackers and the threats they
pose. However, the events that occurred during the Arab Spring and the continual evolution of hacker capabilities indicate that it is not outside the realm of possibility for hackers to acquire cyber-warfare capabilities on par with those of nation-states, especially when there is discussion within the magazine’s community of attacking the NSA itself, an institution with unrivaled computer network exploitation capabilities (justanothersubscriber, 2014).

The hacker community typically rallies against antipiracy legislation. It also believes that the Computer Fraud and Abuse Act (CFAA) of 1986 gives federal prosecutors too much power to facilitate the harassment of hackers. Internet activist Lawrence Lessig (2013) commented, “For 25 years, the CFAA has given federal prosecutors almost unbridled discretion to bully practically anyone using a computer network in ways the government doesn’t like (Lessig, 2013, p. 1).” Boston attorney and writer Harvey Silvergate (2013) described the legislation as “a notoriously broad statute enacted by Congress seemingly to criminalize any use of a computer to do something that could be deemed bad” (Lessig, 2013, p. 1).

In the eyes of the community, hacking and piracy are revolutionary actions, and the community as a whole is anarcho-socialist. They envision and advocate a kind of informal and uncontrollable redistribution of wealth (Woods, 2013). They fight against hyper-capitalism, a system in which the means of production are privately owned and operated for profit and the distribution, income, production, and pricing of goods are determined through a free-market environment independent of government influence to the detriment of the masses (Ile Emi Ifa, 2014). They view hyper-capitalism as a growing phenomenon that they must actively resist, engaging in constant conflict with corporations that seek to protect their copyrighted material.

There is a tendency within the hacker community to be distrustful and suspicious not only of corporations but also of the government; the community is ever fearful that the government
will resort to extralegal harassment of its members. Though there is reasonable cause to be paranoid in oppressive regimes such as China or certain Middle Eastern nations, hackers also fear what they call the “American censorship regime” (LeConte-Spink, 2013).

The hacker community fears that government entities, in collusion with corporations, will resort to such measures as black propaganda; support of network attacks in which members of a hacker’s family are harassed; press hit jobs or public slander; and outsourced thuggery to coerce members of the hacker community to remain silent or desist from their activities. The hacker community lives under the persistent fear that the government will engage in abuses of civil liberties and social violations not seen since the COINTELPRO program conducted by the FBI from 1969 to 1971 (LeConte-Spink, 2013). Indeed, the community is consistently paranoid about government spying and surveillance, both at home and abroad (^SUBv, 2013).

Community members often theorize that most government transgressions are due to the actions of a few who cover for one another in an old boys’ club. They believe that exposing these activities is the surest way to defend themselves against these and other malicious networks. The tactic of publishing information about the government, including its officials, in a secure, non-censorable location is seen as a means of self-protection from extralegal harassment. This reflects the belief that transparency will deter transgressions and that “Sunlight is the best disinfectant” (LeConte-Spink, 2013).

**Viewing DDoS as a Legitimate Form of Protest.** Molly Sauter’s work *The Coming Swarm: DDoS Actions, Hacktivism, and Civil Disobedience on the Internet* examined the ethics of using DDoS attacks. Aligning with ELF and ALF views on property destruction as a nonviolent and legitimate form of protest, Sauter’s work cited the work of Ethan Zuckerman and Doug McAdam as well as an essay on electronic civil disobedience by Critical Art Ensemble to
argue that DDoS is akin to a virtual sit-in and is therefore a legitimate form of protest. Sauter (2014) acknowledged that DDoS attacks violate a sacred tenet in the hacktivist community—freedom of speech—as well as the controversy within the activist community over the use of DDoS attacks as legitimate protest. She quoted notable hacktivists, such as Cult of the Dead Cow founding member Oxblood Ruffin, who consider DDoS attacks to be lazy activism that violates the activist culture of “willful violation of law; deliberate arrest; and having one’s day in court” (Sauter, 2014, p. 5).

Activist culture considers activism to be a strenuous and dangerous undertaking where the activist risks arrest, police brutality, and torture, none of which are risked in DDoS attacks commonly used by hacktivist collectives. Central to the theme of public disruption is the acceptance of punishment. Indeed, as Sauter (2014) pointed out, “Activism has a strong, discernible effect on its target. If the activist is not placing himself or herself in physical danger to express their [sic] views, then it is not valid activism” (Sauter, 2014, p. 6). This constellation of beliefs is widely recognized as being vitally important to civil disobedience activism: it happens in public, and it happens on the street. Activists willingly face consequences, such as arrest or injury, for their cause, thus legitimizing the activist's actions (Sauter, 2014). Hacktivists do not risk such consequences and value their anonymity. Sauter (2014) concluded that DDoS attacks are akin to public disruption techniques, such as sit-ins, and are therefore legitimate forms of protest despite the contradictions between hacktivist and activist cultures.

**Call to Action**

The hacker community, which views privacy as a right, reveled in the disclosure of NSA data collection programs by Snowden, believing that people should never subscribe to “just trust us” reassurances by anyone in authority. Corley (2014) has held up Snowden as a hero and has
attempted to instill a sense of outrage in the community over the NSA’s storing of metadata from half a billion telephone calls and emails from Germany alone every month; the implanting of back doors into consumer products with the help of the tech industry; and the interception of unencrypted communications from Google’s and Yahoo’s data centers. In bringing to light these perceived transgressions, Corley called for hackers to engage in activism to protest these actions, which, in his view, constitute Orwellian surveillance (10cke, 2014).

In its editorial section, 2600 Magazine published the opinion that retaliatory action should be taken against all government officials involved in the Aaron Schwartz case, including the assistant prosecutors, higher officials, and those who filed indictments, to hold them accountable to the public (Corley, 2014). This appears to be a blatant call to action for hacktivists to target and harass these individuals. The editorial’s writer was touching upon the community’s perception that the government responds in a draconian fashion to alleged breaches of ethical computer use, passing and enforcing overly harsh laws and engaging in extreme prosecution and sentencing of hackers when caught.

The April 2014 edition of the magazine published a subscriber’s letter calling for an attack by the collective community of hackers on the NSA to thwart its collection activities. Instead of advising against such an action, as it has in response to previous letters expressing similar sentiments, the editorial staff was silent on the issue and instead offered advice on how users can remain anonymous if engaged in risky, illegal behavior online (justanothersubscriber, 2014).

According to the U.S. Department of Homeland Security, in May 2013, Middle Eastern and North African hackers made preparations to conduct cyber-attacks against the websites of high-profile U.S. government agencies, banks, and other companies in an operation they called
#OpUSA. It was believed that the group was acting in the name of Anonymous. There was an announcement on the electronic bulletin board Pastebin calling for the operation to begin on Tuesday, May 7, 2013 (Waterman, 2013). The attacks planned for May 7 were, however, a failure; no high-profile sites were taken offline, and only a few lesser sites were compromised and defaced (Huang, 2013).

However, the failed attacks provided a glimpse into how such hacktivist groups operate. Forensic investigations led to the discovery that the hackers had accessed and compromised the sites before the target launch date of May 7, 2013. This gave investigators important insights into activist operations; it revealed that a call for an attack on a bulletin board is not indicative of an impending attack, but may suggest the possible manipulation of a system that has already been compromised (Huang, 2013). The attacks also revealed the technical proficiency of the attacking group. Far from being sophisticated adversaries, the hackers involved in the planning of #OpUSA appeared to have only “rudimentary” hacking abilities (Waterman, 2013).

**Combating Cyberterrorism**

Some works, such as Schneidewind’s 2006 article “Solutions to the Threat of Cyber Terrorism to Homeland Security,” have gone so far as to propose methods for fighting cyberterrorism. Schneidewind argued that the United States is currently no more secure than it was in 2000 because attacks on the Internet continue unabated and because there is a pressing need to implement counter-cyberterrorist solutions into homeland security strategies. To that end, he called for several initiatives at the federal level to secure the nation’s critical infrastructure including: software companies must be required to patch and secure vulnerabilities once they are discovered; innovative research in cybersecurity must be funded; the National Strategy to Secure Cyberspace must become technically implemented; and the government must
support university fellowships to produce scientists and engineers who specialize in cybersecurity architecture design (Schneidewind, 2006).

Amin (2008) argued that cyberterrorism differs from other forms of Internet crime such as identity theft and money fraud in that it uses technology to divert or destroy systems and infrastructures and seeks to cause injury or death as a way to undermine economies and government institutions. The more digitally connected a nation is, he asserted, the more vulnerable it is. As the world becomes more wired, it will become increasingly vulnerable to cyberterrorism, and the international community must work together to address this threat (Amin, 2008). In his analysis, Amin (2008) focused on case studies, including the Estonia-Russia conflict in which cyber-attacks shut down Estonia’s water treatment plants, caused massive disruption to its banking system, and wreaked havoc on government agency websites for more than three weeks (Amin, 2008).

Gable (2010) claimed that cyberterrorism will become one of the most significant threats to the national and international security of the modern state. He discussed the difficulties nations face in securing the Internet, the first of which is defining what constitutes an act of cyberterrorism. What some states consider acts of cyberterrorism others would classify as acts of vandalism. Gable postulated that preventing cyber-attacks is not a feasible strategy. Instead, the best strategy is to deter the threat of cyberterrorism by consistently and effectively prosecuting individuals committing acts of cyberterrorism under the international law principle of universal jurisdiction. Gable’s work complemented Genosko’s (2007) analysis of the Canadian hacker Mafiaboy, which illustrated the need for cross-agency cooperation to deter and prosecute hackers whose crimes often cross jurisdictional boundaries both within and between nations.
**Combating Radicalization.** McCauley and Moskalenko (2011) discuss the need to limit political radicalization and the violence that can emerge from radicalization to prevent terrorist campaigns from ever being implemented. Deradicalization is the process of changing a belief system that will encourage individuals to reject extremist ideologies and embrace mainstream values. Government efforts to combat radicalization by attempting to repress it often fail, as repression alone often backfires and causes further radicalization (Rabasa, 2010, p. xv). Governments must take comprehensive approaches to combating radicalization and terrorism. The first step toward preventing the occurrence of terrorism is to understand it. If a government cannot understand why people turn to violence, it cannot hope to stop it, reduce it, or immunize against its effects. Furthermore, if a government cannot understand radicalization, it will have to live with its effects, which include the extremes of terrorism (McCauley & Moskalenko, 2011).

**Legislative Processes to Empower the Government.** The *Washington Post* reported in May 2014 that the Department of Justice (DOJ) is seeking expanded powers to make it easier for the FBI to obtain warrants to hack into a suspect’s computer for evidence when the location of the computer’s physical location is unknown. This proposal came in response to the challenges the bureau faces in apprehending and prosecuting individuals who conduct crimes online using tools to conceal their identities (Nakashima, 2014).

Civil liberties advocates, such as the activist wing of the Electronic Frontier Foundation, fear that the DOJ’s proposal would gradually lead to more invasive searches of a person’s property. They also cite concerns about whether the government would or could target the correct computer when conducting such searches remotely. The measures proposed by the DOJ include the ability to activate a computer’s built-in camera remotely. Were the government to
erroneously target the wrong computer, they could inadvertently come across the private and sensitive information of an individual unrelated to their case (Nakashima, 2014).

On the other hand, granting the DOJ’s request to allow remote hacking of a suspect’s computer would facilitate the apprehension of botmasters (those who run botnets) according to Vatis. He claimed that, in some cases, the only way to determine the location of criminals who may themselves be spreading destructive malware is “to use software that goes across the Internet to reach the originating computer. There’s no reason to prohibit that” (Nakashima, 2014, p. A4). Furthermore, DOJ officials claim that this additional leeway for remote surveillance would make it easier to combat cyber-crimes that cross jurisdictional boundaries. According to Mythili Raman, a former acting assistant attorney general for the DOJ’s criminal division officials say that investigations often require law enforcement to act in many jurisdictions at one time in the case of botnets. Coordinating simultaneous warrants in multiple districts may not be possible as a practical matter. The proposal remedies this, and yet still requires that prosecutors show probable cause to obtain a warrant and that the items to be searched and seized be described with “particularity.” At the time of this writing, the proposal is still undergoing congressional review processes (Nakashima, 2014).

**Feasibility of Deterrence.** In “Cyberdeterrence and Cyber War,” Martin Libicki (2009) discussed the realities of attempting to implement strategic policies of deterrence to thwart cyber-attacks. In Libicki’s opinion, deterrence is not a practical option, as cyberspace is a unique domain in its own right. As a result of issues of attribution, it may not be readily apparent who the attacker is, meaning that the retaliator could potentially fall prey to a red flag operation and retaliate against the wrong target and thereby creating a new adversary. Another issue with attribution in cyberspace is that the target may not even realize that it is under attack. Systems
today are becoming more and more complex. Simpler systems are not necessarily more vulnerable to attack in comparison to complex systems. In fact, simple systems may be more immune to attack, as it is easy to identify when something has gone wrong. With complex systems, it is not readily apparent when something is wrong, and it is often even more difficult to identify the source of the problem. In highly complex systems, it may not even be readily apparent that the cause of the problem was a computer network attack (Libicki, 2009).

In the case of many cyber-attacks, attribution takes time, delaying a state’s retaliation to the point to where it could appear that the retaliation is a new attack, bringing about counter-retaliation. Further complicating matters is that a state with a publically declared deterrence policy might decide to hide that it was attacked to avoid being boxed into taking a retaliatory response as called for in its deterrence policy, as well as to avoid looking inept (Libicki, 2009).

**Waging Cyber-War: Readiness and Sustainability.** Libicki (2009) also discussed the issues of readiness and sustainability of forces when fighting a war in cyberspace. Regarding readiness, Libicki argued that it is not possible to maintain a constant state of readiness within cyberspace, as it is within other domains. In cyberspace, the attacker and would-be retaliator must both maintain an arsenal of different tricks because technology is evolving so rapidly that what works one day may not work the next. Defenders develop patches against exploits, and attackers develop new techniques. Furthermore, a state cannot necessarily develop, exploit, and hold cyber exploits in reserve for future action, as the would-be target can become aware of the vulnerability and develop a patch to negate its effects (Libicki, 2009).

When developing force structure, it would be best to have a cadre of elite hackers that develop the zero-day exploits that would be used operationally. More is not necessarily better when it comes to the use of hackers in cyber-warfare. There are not many elite hackers, and the
overuse of second-tier hackers using known exploits would not only deplete the use of available cyber-weapons, but also they could serve to immunize the target against further attacks (Libicki, 2009).

Meanwhile, sustaining a cyber-conflict is an issue unto itself. Libicki (2009) stated that operationalization of cyber-warfare is of limited use because once an exploit is used in the initial stages of conflict, the target can take steps to reduce its effects and begin configuring its firewalls to block the exploit entirely. Air-gapping systems and other defense measures can be deployed also. Indeed, victory is about which side can take more of a pounding when it comes to conflict in cyberspace. Therefore, Libicki concluded, it is in a state’s best interest to dedicate the bulk of its cyber-war personnel to defense; states should subsidize the education of information security professionals to best prepare for the possibility of conflict.

The findings of Craig Timberg and Lena Sun in their analysis of U.S. government spending on information services, published in an October 2013 Washington Post article, support Libicki’s recommendation. Timberg and Sun (2013) found that the U.S. government spends more than $80 billion annually on information technology services for systems that are becoming ever more complex, take years to build, and are outdated by the time they launch. Furthermore, throughout the federal government, there is a lack of trained technical staff to operate and maintain these systems, much less keep them properly configured and secured, highlighting the need for additional security professionals.

**Indications and Warning (I&W).** Warning intelligence, commonly referred to as Indications and Warning (I&W) Intelligence, is a post-World War II system intended to prevent surprise attacks such as the Japanese attack on Pearl Harbor. It was further developed in response to fears of a military surprise attack from the Soviet Union (Grabo, 2010).
I&W relates to pieces of information about what an adversary might do. It is a risk assessment of the threat posed to government assets by various sources. The product of I&W is a research effort that assesses what an adversary might do and assigning probabilities to each likely course of action. The final product is a probability assessment that gives policymakers a reasonable insight into probable enemy actions, allowing them to more confidently make decisions (Grabo, 2010; Wallace & Webber, 2011).

One aspect of counterterrorism is the monitoring of suspected terrorist groups to develop a risk assessment of the threat and prevent or protect against an attack (Wallace & Webber, 2011). In training intelligence analysts on the art of I&W, the curriculum at the Joint Military Training Center urges analysts to adopt a mindset that focuses on the threat, the use of both analysis and synthesis, the use of probabilities and possibilities analysis, and opportunities to counter the threat(s). According to Joint Military Intelligence Training Center curricula, there are two types of warning: emerging and enduring. The emerging warning is a scenario of a potential threat to U.S. interests and national security that does not yet exist but has the potential to develop. An enduring warning is a warning regarding monitored threats to U.S. interests and national security that presently exist. Emerging warning problems, once they become reality, turn into enduring warning problems (Joint Military Intelligence Training Center, 2014). The U.S. government could consider adopting the U.S. Department of Defense Joint Staff’s emerging warning construct to address the potential threat of hacktivists becoming cyberterrorists. The benefit of adopting such a construct would be to provide government entities with adequate lead time to defend networks against impending attacks.

There are five steps to an emerging warning problem that are intended to identify an anomaly from a broad field and generate scenarios from a range of plausible potentials: 1)
determine the cone of plausibility, 2) sort out which scenarios to explore, 3) determine if there is a warning message in any of the scenarios, 4) identify or review, and 5) explore opportunities (Joint Military Intelligence Training Center, 2014).

The steps of warning are complemented by the stages of warning identified in Grabo’s *Handbook of Warning Intelligence* (2010). The first step, the cone of plausibility, involves the collection of data. During the cone of plausibility phase, the analyst collects data that fit into categories or drivers that fall within either the PMESII-PT (political, military, economic, social, information, infrastructure, physical environment, time) or STEMPLES (social, technical, environment, military, political, legal, economic, security) construct. The collection of data and their subsequent categorization is known as *environmental scanning*. Once the data are categorized, each category or driver is ranked, depending on the analyst’s assessment of which drivers take precedence for the adversary and motivate that adversary to take action (Grabo, 2010; Joint Military Intelligence Training Center, 2014).

The second step of sorting out which scenarios to explore involves winnowing down the mass of incoming information to identify if there is a warning issue that poses a threat. If there is such a threat, the analyst must also identify its potential impact and implications, as well as question the possibility of deception. In this step, the analyst identifies, at a minimum, three possible scenarios about the course of action the adversary might take based on its drivers. The first scenario is predicated on the assumption that the adversary will continue to act as it has always has. The second scenario takes into account the anomaly or anomalies that have affected one or more of the drivers that are behind the course of action the analyst believes is likely. The final wild card scenario involves a course of action the analyst does not believe is likely but that
could occur considering all the drivers (Grabo, 2010; Joint Military Intelligence Training Center, 2014).

The third step of determining if there is a warning message in any of the scenarios involves the evaluation of indicators to determine if a warning message is warranted for any of the scenarios identified in stage two. If a warning message is warranted, analysts are required to identify the scenario as well as provide a brief explanation of why they do not believe any of the other scenarios are likely (Grabo, 2010; Joint Military Intelligence Training Center, 2014).

The fourth step, identification and review, involves an assessment of the warning indicators. In this step, analysts review the conditions and drivers necessary for the likely scenario to occur, as well as the assumptions and factors that influenced those conditions. This step also involves identifying any indicators that show that the conditions are coming into play and will lead to the likely scenario (Grabo, 2010; Joint Military Intelligence Training Center, 2014).

The final step of exploring opportunities involves the identification of opportunities and those actions that could be taken to exploit them. Complementing Grabo’s final stage of warning, this step also involves conveying, through a paper or brief, the possible consequences that could occur if those opportunities were exploited (Grabo, 2010; Joint Military Intelligence Training Center, 2014).
Figure 2. Plausibility Limit. This figure illustrates the cone of plausibility in developing scenarios. Adapted from Joint Military Intelligence Training Center. (2014). Indications and Warning.
Indicators. Cyber-reconnaissance is an indicator of an impending cyber-attack. It is conducted in three basic steps: footprinting, scanning, and enumeration. Footprinting is the examination of the structure of an organization’s computer network. It involves obtaining network information including the range of IP addresses, the addresses of key network equipment such as routers, the availability of remote access to the network, and the presence of network-level security devices such as intrusion detection systems and firewalls. Scanning involves examining the network in more detail, going beyond the measures used in footprinting. In this step, the details of the system, such as what operating system is being used, are determined. This is also when the intruder determines what ports are open. Enumeration involves the interrogation of specific systems; the intruder often tries to log into a system in an attempt to find specific data. The goal of this step is to determine any vulnerability in the system that might allow the intruder to obtain access. Software that may allow enumeration includes Crawl Web site, DumpSec, NetBIOS Auditing Tool, and Network Scanner (Shakarian, Shakarian, & Ruef, 2013).
Summary

The exact extent of the threat posed by cyberterrorism is debatable, largely because there has not yet been a recorded case of cyberterrorism that has been verified. However, there is some consensus within the security community and beyond that the formative stages of cyberterrorism are already being expressed within communities of patriotic hackers and hacktivists. Members of these groups are theoretical precursors to cyberterrorists, just as many patriots and activists in the material, non-digital world have radicalized and become terrorists in the past.

The focus of the study will be to collect information from various entities to answer the question, “are hacktivists radicalizing and becoming potential cyber terrorists?” The research will further explore the concept of cyberterrorism and the potential ways extant groups and actors could become cyberterrorists. The study will also explore opportunities in the form of new policies, laws, and collaborative government initiatives to combat this potential threat.
Chapter 3: Research Methodology

Background

Unlike its tactical situation in other domains—land, air, sea, and space—the United States does not possess superior force in cyberspace. The Internet is a contested domain, and the United States has not yet discovered a way to operate with impunity within it while maintaining plausible deniability about such capabilities with its adversaries. The Internet has a very low barrier to entry. For a few thousand dollars, any individual, group, or state can become an important actor in cyberspace.

The United States relies heavily on the unimpeded use of cyberspace not only to conduct military operations but also to support its banking industry and critical infrastructures. The original Internet design was for a system optimized for information sharing and did not have security in mind. Such concerns were an afterthought, and many commercial vendors still do not see much of an economic incentive to design code that is secure at its inception, often resorting instead to the release of aftermarket “patches” to correct vulnerabilities as they are discovered. These patches are often created or implemented by technologically adept members of the software’s user base, who, ironically, are likely to be members of the hacker community as well.

According to the Diplomatic, Information, Military, and Economic (DIME) paradigm, the combined result of these practices in the information technology (IT) community and U.S. dependence on cyberspace is that there are now several weak points in U.S. national security. The Russian conflict against Estonia, an instance where cyber-attacks crippled national response capabilities, demonstrated the havoc that cyber-attacks that non-state actors can wreak (North Atlantic Treaty Organization, 2010).
The weapons of terrorism are evolving to keep pace with technology, just as they always have. In the days of the Sicarii, a group of Jewish extremists in the ancient Roman province Judea in the first century that violently opposed Roman rule, terrorists used knives and daggers. The term Sicarii is derived from the Latin word sicarius, which means ‘assassins’ or ‘murders.’ The Sicarii were known as ‘dagger men’ and used short daggers to carry out assassinations. Their primary targets were Jewish collaborators (Zalman, 2014). In Czarist Russia, anarchist extremists fighting for social and political change used rudimentary explosives. On 9/11 in the United States, we saw terrorists use airplanes as guided missiles. Today, terrorists are using the Internet more than ever before to plan operations, spread propaganda, and conduct attacks in cyberspace.

The hacking community has its own unique culture, one that emphasizes openness and freedom of information. Over the years, it has expanded and diversified to include other subgroups including hacktivists who conduct cyber-attacks on governments and other organizations as a form of political protest. It is likely that many hacktivists, particularly those who are also Islamic extremists, will, at some point, radicalize and begin to use cyberterrorism to further their political objectives.

**Research Design**

The design of the research is to explore the reasons why hacktivists have yet to resort to acts of cyberterrorism and the likelihood that they will do so. With a pragmatic approach using a case study design, this study will examine the terrorist-evolved use of information technology ranging from chat rooms and message boards to virtual reality environments such as Second Life, an online virtual reality community created by users, which could be used for training and the rehearsal of attacks. Any of these platforms could also be used to coordinate cyberterrorist
activities. In this study, the researcher will also analyze cyber-attacks that have occurred over the past seven years. This will include the attacks in Estonia and the distributed denial of service (DDoS) attack on American Express on March 28, 2013 for which the so-called “cyber-fighters” of Izz ad-Din al-Qassam have claimed credit. This study will also analyze the many attacks that have occurred since September 19, 2013, on Bank of America, JP Morgan Chase, Wells Fargo, U.S. Bank, and PNC Bank (Rothman, 2013; Soulskill, 2013).

**Sampling**

The sampling methodology will be a non-probabilistic, purposive method, a method that purposively selects a target population exhibiting specific characteristics including individuals involved in hacktivist organizations and who use information technology and cyberspace as mediums for expression and political activism. It will examine cases in which these groups and individuals have resorted to hacking websites and engaging in other types of cyber-attacks, such as DDoS attacks, on targets whose policies and practices they protest. To ensure external validity, the study will utilize the proximal similarity model when sampling hacktivist organizations and individuals who operate in cyberspace and will examine terrorist organizations that began as activist and patriotic organizations whose ideologies later radicalized and escalated to the point of using violence to pursue their objectives (Web Center For Social Research Methods, 2013).

**Measuring Instruments**

This researcher measured samples from the past three years in the following categories:

1. The number of attacks reported by Internet service providers (ISP), companies, banks, and government agencies. The types and sources of the attacks will be examined to assist in conducting a trend analysis of the targets of hackers and hacktivists, the types of attacks employed, and their impact on targets.
2. The attacks that hackers and hacktivists claim credit for on the Internet and the nature of those attacks. Sources of information include hacker blogs such as 4chan, chat rooms, and social media sites such as Twitter, YouTube, and Facebook. Answering this question provided insight into the motivations and beliefs of groups likely to resort to cyberterrorism.

3. The means by which terrorist organizations employ the Internet to support their operations. This ties into the first question posed by the study as it relates to the expertise and maturity of the organization as an actor in cyberspace.

**Data Collection Procedures**

Data were collected from publicly available sources; this included reports of attacks, such as the CISCO Annual Security Report (CISCO, 2013). The study will also include observations of hackers, via online IRC chat rooms, hacker club meetings, and conferences. Data were also collected from the observation of individuals who conduct cyber-attacks, such as “reformed” hackers who now operate as legitimate “white hat” hackers and hackers (via trolling Internet forums) who boast of their cleverness in being able to penetrate their target networks as part of a propaganda analysis: reports of new trends and developments. Hackers are known to occasionally share nicknames to help obfuscate their identities or even flat-out lie (Olsen, 2012, p. xi). This makes identifying sources very difficult. Propaganda reflects concern and most propaganda contains some truth. Propaganda warning is usually indirect rather than specific (Grabo, 2010). Due to the frequent practice of multiple users sharing and changing nicknames, and considering that most propaganda contains some truth, it will be assumed that the
information conveyed by online personas attempting to coordinate and conduct cyber-attacks are being truthful with their intent, although their individual capability cannot be verified.

To obtain data regarding existing terrorist organizations, the researcher collected information on known terrorist websites, chat forums, and online databases, along with the means, methods, and purposes by which these organizations employ Internet technologies. Information was captured in Excel files and was collected using non-attributable searches by hiding the researcher’s source IP address using free and open source technologies such as The Onion Router (TOR) browser, and free online proxy services such as hidemyass.com. The TOR browser and hidemyass.com are technologies commonly used by individuals, such as government officials and celebrities, for the purposes of searching the Internet anonymously and for privacy concerns. The use of typical search engines, such as Google and Yahoo, collect information regarding an individual’s search queries and do not hide the individual’s source IP address, leaving open trails of their identity.

Data Analysis

One of the main challenges in collecting data for the research is that companies—banks, in particular—are reluctant to report that they have been the victims of cyber-attacks because of their fear of losing customers. A retro-analysis of corporations that offer anti-hacking services and the average revenues they receive will allow for extrapolation of the overall funding that corporations allocate toward cyber-security.

Qualitative analysis of the samples gathered and a trend analysis using nodal network analysis will be used to identify patterns in reference to the type and nature of attacks conducted against government and financial institutions by hacktivist organizations. In addition, the

---

3 Online persona is the identity an individual or group creates and uses in cyberspace.
researcher will utilize a qualitative analysis of hacktivist organizations’ use of Internet technologies, by examining free cyber-weapons they disseminate to attack targets, and the processes they follow in comparison to the evolution of weapons that radicalized activists turned terrorists have employed to fulfill their political agendas. Data will be presented in charts, graphs, and tables.

Assumptions and Limitations

The primary assumptions entering into this study are:

1. The United States does not possess a force in cyberspace capable of achieving supremacy and continues to rely on information technologies that possess vulnerabilities. Therefore state, and non-state actors, have the ability to challenge U.S. operations in cyberspace, and influence DOD operations that rely upon cyberspace.

2. Any individual, group, or state can become an influential actor in cyberspace. Therefore, any individual, group, or state can influence DOD operations that rely depend open lines of communication in cyberspace.

3. Like Hackers, hacktivists interact and socialize virtually instead of in person. Like activists, they can radicalize from their participation and interaction with like-minded individuals and become extremists. It is possible that hacktivists can radicalize from their virtual social interaction and participation with like-minded individuals, and, once radicalized, hacktivists will conduct acts of cyberterrorism against government targets.

4. The researcher will be able to successfully gain access to the hacker community, and observe truthful information about its illicit activities and its future intentions.
The limitations of the study are that it will attempt to generalize the population of hackers and hacktivists, and that it may be unable to keep pace with evolving technologies, tools, and techniques that hacktivists employ to counteract evolving cyber-security measures.
Chapter 4: Data Analysis

Case Study Analysis: Evolution of Cyber Conflict

Cyber conflict has evolved over time; however, in many respects, the threats posed are the same that existed in the 1980s. The following case studies illustrate the historical time line of the impact and magnitude of the cyber threats to U.S. national security:

- Cuckoo’s Egg (1986)
- Morris Worm (1988)
- Russian Patriot Hacking/Chinese Patriot Hacking/India and Pakistan Patriot Hacking (1994-2011)
- Eligible Receiver and Moonlight Maze (1997)
- Solar Sunrise (1998)
- Russian Versus Estonia Cyber Conflict (2007)

**Cuckoo’s Egg.** This case illustrates the point that a hacker may not always be interested in stealing classified data but rather may seek to acquire virtual resources to aid in conducting follow-on cyber operations against other targets (Stoll, 1989).

Clifford Stoll was not aware of a security breach at the Lawrence Berkeley Lab, located at the University of California, Berkeley until he investigated the source of a 75-cent shortfall in computer time billing in August 1986. In June 1987, Stoll completed his investigation. What he eventually uncovered was that a hacker, Markus Hess from West Germany, was applying his skill set as part of an espionage ring in Germany to sell Western technological information and secrets to the Soviet Union (Stoll, 1989).

Hess hacked into an unsecured MITRE computer, which allowed him access to the company’s network (the rest of the computers in the company were secured). From there, he hacked into other locations, including MILNET and military networks. The hacker was able to invade many systems, including those of the military, because system administrators failed to
password protect their user accounts. Following this incident, the U.S. government became more security conscious (Stoll, 1989).

This case delineates the issues in battling these sorts of wrongdoing. Stoll (1989) needed to work with the Department of Energy; the Federal Bureau of Investigation (FBI), which chose to dismiss him; the U.S. Armed Force Criminal Investigative Division (CID); the Air Force Office of Special Investigations (AFOSI); the Defense Communications Agency, which is currently a part of the Defense Information Systems Agency (DISA); the National Security Agency (NSA); the Defense Intelligence Agency (DIA); and the Central Intelligence Agency (CIA). Each agency had to respond with care to avoid crossing into another agency’s jurisdiction (Stoll, 1989).

This case also highlights the difficulties in coordinating efforts with foreign services in apprehending hackers overseas. The FBI was lethargic in its domestic response and continued to be when coordinating with officials of the German federal post office in arresting Hess (Stoll, 1989).

This case study also illustrates how resource intensive the process is to catch a hacker. The primary challenge is that hackers usually have to be active for a while and commit repeated offenses before they can be caught. While investigating the hacker in this particular case, Stoll and his colleagues discovered that the individual altered the operating system of a medical program used to control the radiation doses cancer patients receive for treating brain tumors. He did this in the attempt to create additional vulnerabilities so that he could enter the laboratory’s network whenever he wished. The altering of the operating system software could have affected the performance and accuracy of the machine administering the dosages of radiation to patients, and posed a hazard that could have resulted in deaths. The hacker also broke into computers that
contained patient records. Had his intent been to harm them, he could have altered their diagnoses (Stoll, 1989).

**Morris Worm.** On November 2, 1988, Robert Morris Jr., a graduate student in software engineering at Cornell, released a trial worm that exploited an opening in the debug mode of the Unix sendmail program into the Internet from the Massachusetts Institute of Technology (MIT). Morris chose to upload the worm from MIT to obfuscate the worm’s origin at Cornell University (Kehoe, 2012). A worm is more powerful than a virus and does not require a user to operate it. At the point when a worm gets access to a machine, it dispatches a program that hunts down workstations at other Internet areas and contaminates them (Schmidt & Darby, 2012).

After Morris uploaded the program, it quickly replicated, infected, reinjected, and crashed many machines around the United States (Kehoe, 2012). By November 3, 1988, Sun machines across the United States were overloaded by tasks the worm commanded, and prevented users from being able to operate the machines and forced system administrators to cut off Internet connectivity entirely in an attempt to eliminate the source of the infection (Schmidt & Darby, 2012).

To resolve the issue, Morris solicited the assistance of a colleague at Harvard University, and the two sent an anonymous message from Harvard educating software engineers on the most proficient method to destroy the worm and forestall reinfection. By the time the two sent the message, infected computers around the country—including at universities, military installations, and medical research universities—had already clogged the network. They did not send the message in time. Damage estimates at each site ranged from $200 to over $53,000 (Kehoe, 2012). In 1988, the Internet was still very small, without commercial traffic or websites; the worm’s harm was limited to analysts at government offices and colleges and a handful of
enterprises that utilized systems to exchange email and other records. It was the first great worm attack (Marsan, 2012).

**Russian /Chinese /India and Pakistan Patriot Hacking.** In 1994, the Zapatista National Liberation Army launched a guerilla war in Mexico. The Zapatistas conducted cyber-attacks that targeted Mexican police websites, the Frankfurt Stock Exchange, and several sites in the United States with the aid of European hackers in 1998. This was the first recorded instance of a cyber militia taking part in a regional conflict (Dudney, 2011).

Most of the cyber-wars that have occurred since 1998 have originated from local clashes. Moreover, they have not been the work of nation-states, but instead unorganized civilian groups, also known as collectives, that organized crime organizations would aid from time to time. These are ethno-nationalists, not members of governments, who conduct aggressive and extensive cyber campaigns. However, these civilian operations often have the tacit support of governments (Dudney, 2011).

Since the Zapatista operations, nearly all regional conflicts that have occurred have had cyber components. When India conducted a nuclear test in 1998, nongovernment Pakistani ethno-nationalists attacked an Indian cyber target. This ignited a cyber campaign that continued for months. In 1999, a digital war occurred regarding the long-running clash in Kashmir. It again involved the digital civilian armies of Pakistan and India with government help on both sides. In the Middle East, the Iranian-sponsored group Hamas assaulted Israeli digital targets. Digital assaults have been persistent features of the Arab–Israeli pressures in the Middle East ever since (Dudney, 2011).

Cyber militias can affect U.S. forces and trading operations. In 1999, the United States mounted cyber-attacks during Operation Allied Force (OAF) over Serbian airspace.
U.S. actions prompted a counterattack by nongovernment Serb actors and eventual participation by Russian hackers. During the kinetic phases of the conflict, a U.S. Air Force B-2 mistakenly bombed the Chinese embassy in Belgrade. Chinese cyber militias responded to the incident by launching a cyber campaign against U.S. targets. Pro-NATO hackers retaliated with counterattacks on Chinese targets. Later, in Operation Unified Protector, the NATO coalition conducted operations to enforce a no-fly zone over Libya in 2011 to implement United Nations (UN) Security Council Resolutions 1970 and 1973. During this operation, there was a battle in cyberspace between Libyan rebels and loyalist forces; one side (the rebels) required the Internet to communicate with the rest of the world while the other side (the loyalist forces) needed to prevent enemy use of the Internet. In this regional conflict, a cyber cat-and-mouse game was played, with the opposition attempting to show the world the atrocities of the Gaddafi regime, and the loyalist forces desperately trying to squash any negative sentiment toward the dictator (Cenciotti, 2011; Dudney, 2011).

A big concern is that governments will not always be able to control the actions of its cyber militias, who thus far have exercised restraint but who may choose not to do so if conflicts escalate (Dudney, 2011).

**Eligible Receiver and Moonlight Maze.** Eligible Receiver is the code name of a 1997 inward practice launched by the Department of Defense (DOD). A red team of hackers from the National Security Agency (NSA) was assembled to penetrate the Pentagon computer network. The red team was permitted only to utilize publicly accessible computer equipment and software. Using only publicly available assets, the team was able to penetrate and take control of the Pacific Command (USPACOM) networks in addition to power grids and 911 emergency systems in nine major U.S. cities (Public Broadcasting Service, 2012).
Hamre (2003) noted the following regarding this exercise:

During Eligible Receiver, the success of the red team was only one-tenth of 1 percent, but that’s enough to get control of the entire network…Pristine protection, absolute sanitary protection, is what’s required, and you’ll never get it.

It’s not about getting sick. It’s about how do you recover your health. (Public Broadcasting Service, 2012, p. 1)

A cyber-war might be hard to detect at first. Often, attackers are unnoticed. In fact, most intrusions are not noticed, as in the case of Moonlight Maze. Moonlight Maze refers to an event in which U.S. officials inadvertently discovered a pattern of reconnaissance of computer networks at the Pentagon, the National Aeronautic and Space Administration (NASA), the Energy Department, universities, and research laboratories. Their investigation revealed that the probing had been ongoing for more than two years, beginning in March 1998 where tens of thousands of files had been exfiltrated. The DOD attributed the exploitation to a mainframe computer in the former Soviet Union, but it is unknown to this day which entity sponsored the attack, and Russia denies any involvement (Arquilla, 2003; Public Broadcasting Service, 2012).

**Solar Sunrise.** When the United States was preparing to take military action against Iraq in response to UN weapons inspections violations, three teenagers initiated a series of computer network attacks against DOD systems from February 1 to February 26, 1998 that became known as Solar Sunrise. The teens attacked the DOD’s unclassified networked computers using a well-known operating system vulnerability in an attempt to disrupt military deployments and operations. They followed the following pattern: (a) probing to identify existing vulnerabilities, (b) exploiting the vulnerabilities, (c) implanting a program (*sniffer*) to gather data, and (d) returning later to retrieve the collected data (Global Security.org, 2013).
No less than 11 assaults used the same profile and targeted Air Force, Navy, and Marine Corps computers around the world. Assaults were boundless and seemed to originate from destinations placed in Israel, the United Arab Emirates (UAE), France, Taiwan, and Germany. Albeit all DOD-targeted systems attacked were reported as unclassified, many of those systems targeted were key support systems, such as the Global Transportation System and the Defense Finance System (Global Security.org, 2013).

The DOD established 24-hour emergency watches, installed intrusion detection on key nodes, and supported law enforcement by providing computer forensics and investigation support. Solar Sunrise substantiated Eligible Receiver findings: The DOD lacked an effective indication or warning system (Global Security.org, 2013).

**Titan Rain.** Titan Rain was the code name federal authorities gave to a cyber espionage ring of Chinese hackers that targeted defense contracting firms, national laboratories, and the World Bank (Thornburgh, 2005). The hackers tried to acquire as many files as possible by penetrating computer networks at U.S. military bases, defense contractors, and aerospace companies (Thornburgh, 2005).

The hackers would typically toil quickly and with a sense of purpose, often commandeering covert sections of a hard drive, compressing as many files as they could manage, and transmitting the data to transit points in South Korea, Hong Kong, or Taiwan before sending them to their final destination in China. Once compromising the network, the hackers took measures to erase traces of the network exploitation and would often leave back doors so that they could reenter the system at will. A complete attack took 10 to 30 minutes (Thornburgh, 2005). Federal authorities learned from Shawn Carpenter, a volunteer midlevel computer
network security analyst working at night to track the intruders, that the attackers were located in
Guangdong, a southern Chinese province (Thornburgh, 2005).

In cyber espionage, it is rare that authorities are effective at identifying or locating the
perpetrators’ country of origin. Hackers may be able to enter a supposedly secure network
easily, but if U.S. federal officials want to track them and prosecute them, they must do so
through a burdensome legal process (Thornburgh, 2005).

As cyber espionage grows, critics of the FBI claim that the agency lacks a sufficient base
of personnel with the requisite technical skills to track foreign hackers, and administrative rules
of engagement often constrain their abilities. This capability gap is at times filled by cyber
vigilantes such as Carpenter. The FBI would require diplomatic-level authorization to perform
actions similar to those of Carpenter (sneaking into foreign computers) without the risk of
sparking an international incident (Thornburgh, 2005).

**Russia Versus Estonia.** This incident highlights the impact cyber operations can have on
a nation. The Estonian case raises awareness that the NATO alliance needs to include cyber
security in its charter and defense doctrine. No single country can singly protect its electronic
resources, and a county defending its electronic resources must cooperate with other nations in
order to do so. However, international conventions that regulate cyberspace currently treat
civilian and commercial cyber security issues as separate matters (Laasme, 2011).

Prior to April 2007, the primary concern of NATO nation members was the protection of
their sovereign network systems without recognizing the need to assist fellow NATO members
in defending theirs. After the attack on the Estonian electronic infrastructure in April and May
2007, NATO prioritized boosting the cyber-defense capabilities of its members (Laasme, 2011).
Estonia, with a population of approximately 1.3 million, is a small country that is considered the nation most dependent on information technology in the world. It is the birthplace of Skype, and most commerce interactions occur over computer networks and mobile devices. Estonia is second only to the UAE in mobile phone subscriptions, with each person in Estonia owning at least one device. Most everyday activities are completed over the Internet, and most of the country is covered by a free Wi-Fi network because Estonians consider Internet access a basic human right (Laasme, 2011).

Estonia’s Internet dependence has brought the nation not only technological freedom but also various defense and security risks. The national security of the nation was threatened in April 2007, when a botnet attacked the electronic infrastructure of Estonia. The only defense Estonian information technology (IT) managers could muster was blocking the international connections to the servers (Laasme, 2011).

Estonia’s electronic infrastructure was attacked by almost one million computers simultaneously. Most of the attacks emanated from hijacked computers within the United States (assumingly by unknown elements inside Russia). The Russian government has denied any involvement with the attacks but suspiciously lacked an expressed interest in searching for the cyber-terrorists responsible for the attack within its borders. More troubling, this case study implies that a non-state actor exists within Russia with the capability of devastating the electronic infrastructure of a state (Laasme, 2011).

Cyber-war can occur between governments and non-state actors and can be financed by states (Laasme, 2011). Cyberspace offers any actor with Internet access three advantages in a conflict: Actors can choose the scale of their organization, the proximity of their targets, and the precision of their attack plans. There are five advantages cyberspace offers an attacking force:
reach, free fire at will, mass targets, easy stealth, and a near instantaneous high-capacity payload (Demchak, 2011).

**Hacktivist Trends**

Social community sites such as Wikipedia, hacker blogs and websites, bulletin boards, print publications, and other media outlets contain information regarding hacktivist attacks over the past two decades. Much like the leadership and members of their historical activist predecessors, the ELF and the ALF, members of one hacktivist (online collective activist) organization can be, and likely are, members of another collective organization. Indeed, members of the Lulzsec and AntiSec groups were active members of Anonymous (Best & Nocella, 2004; Olsen, 201). By nature, hackers continually change their online personas, use multiple personas, and impersonate the online personas of others. This characteristic, combined with the collective nature of hacktivist communities in which members join, participate, and leave at will, means that it is often difficult to determine the true source of an action or attack. Therefore, an assumption of this study is that the collective group claiming responsibility for an attack is the true attacker, at least in propaganda analysis terms. The following is an analysis of recorded activities of several collective groups from the 1990s through 2013, used to determine current trends of attacks committed by hacktivist organizations:

- Cult of the Dead Cow
- Syrian Electronic Army
- pHC
- giest
- ~EL8
- Naija Cyber Hacktivists
- Anonymous
- People’s Liberation Front
- Cutting Sword of Justice
- Thehacker12
- AntiSec
- Lulzsec
- Redhack
Table 2 describes the key used to code collected data pertaining to hacktivist attacks from the 1990s though 2013. Attacks are categorized by the actions taken by the hacktivists, the targets of the attack, and the motivations and objectives of the attack. Specific attacks of each of the hacktivist collectives identified from 1990–2013 are listed in Tables 6–18.
<table>
<thead>
<tr>
<th>Action</th>
<th>Definition</th>
<th>Sector</th>
<th>Definition</th>
<th>Objective/Motivation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Harassment</td>
<td>Unprovoked attack</td>
<td>Corporate</td>
<td>Corporation or business</td>
<td>Internet Vigilantism&lt;br&gt;Attempting to effect justice according to the groups' understanding of right and wrong.</td>
</tr>
<tr>
<td>Retaliation</td>
<td>Response to perceived slight or perceived unjust practice that negatively influences the social online community. Typically a response to an action that involves an insult to a member of group of Anonymous or a threat to the open sharing of information or free speech.</td>
<td>Private Person</td>
<td>Individual person</td>
<td>Victimizing&lt;br&gt;Turning a person, organization, government, or other entity into a victim of an unprovoked attack.</td>
</tr>
<tr>
<td>Support</td>
<td>Logistical support to a cause that is in line with the group’s core values of equality, transparency of government and corporate governance, the freedom of information and freedom of speech</td>
<td>Religious Entity</td>
<td>Organized religion</td>
<td>Deterrence&lt;br&gt;Attempt to dissuade a person, corporation, organization, or government entity from taking an action not yet started or from taking such action again.</td>
</tr>
<tr>
<td>Social Justice</td>
<td>Seeking to take action against an individual, group, or entity engaged in reprehensible practices.</td>
<td>Social group</td>
<td>Private organizations and associations</td>
<td>Coercion&lt;br&gt;Attempt to influence person, group, organization, or government into taking action or adopting practices preferred by the hacktivist organization.</td>
</tr>
</tbody>
</table>

Note. Source: author
Figure 3 illustrates the number of attacks that occurred from 1990–2013. The majority of attacks occurred in 2011, though a sizable number took place in 2013.

Figure 3. Number of Attacks From 1990–2013. This figure illustrates the years when hacktivist collectives were the most active.
Complementary to Figure 3, Figure 4 illustrates the numerical trends of hacktivist attacks, which is in relative decline from its peak in 2011.

![Numerical trends of attacks from 1990-2013](image)

Figure 4. Numerical Trends of Attacks From 1990–2013. This figure illustrates the peak of hacktivist activity which was in 2011.

Figure 5 illustrates an increasing trend of acts of harassment by hacktivists, along with actions intended to enact social justice.
Figure 5. Hacktivist Acts, by Apparent Purpose. This figure illustrates the increasing trend of hacktivist harassing entities.

Since the peak of activity in 2011, the goal of hacktivist attacks has apparently been to victimize the groups’ targets; the hacktivists are also using Internet vigilantism to enact social justice.
Figure 6. Objectives and Motivations of Hacktivist Groups. This figure illustrates and increasing motivation of hacktivists to coerce and victimize their targets.

Perhaps more relevant, and certainly more cause for concern, especially with respect to the third hypothesis of this study, is the selection of hacktivists’ targets. Hacktivist attacks are increasingly targeting government entities, as shown in Figure 7. This graph is an indication that governments should be concerned about the possible radicalization of hacktivist groups. A related concern is the creation of radical splinter groups by hacktivists unsatisfied with their current collective, who may form their own collective and choose to employ acts of cyberterrorism to achieve their objectives.
Figure 7. Trends of Hacktivist Attacks. Hacktivists are increasingly targeting government entities.
Table 3. Summary of Hacktivist Collectives Analyzed.

<table>
<thead>
<tr>
<th>Group</th>
<th>Description</th>
<th>Years Active</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cult of the Dead Cow</td>
<td>A hacking club that develops and provides Internet privacy and security tools to political activists. (Cult of the Dead Cow, 2014).</td>
<td>1990-2002</td>
</tr>
<tr>
<td>~EL8</td>
<td>One of the first anti-security hacker groups formed (Wikipedia, 2014c).</td>
<td>2002</td>
</tr>
<tr>
<td>Naija Cyber Hacktivists</td>
<td>Nigerian based hacktivists dedicated to exposing corruption, fraud, and abuse within the Nigerian government (Ogala, 2011).</td>
<td>2011</td>
</tr>
<tr>
<td>AntiSec</td>
<td>Hacktivist collective which was an offshoot of Anonymous, opposed the computed security industry (Wikipedia, 2014c).</td>
<td>2011</td>
</tr>
<tr>
<td>Lulzsec</td>
<td>Blackhat hacker group, which was another offshoot of Anonymous, that targeted corporate and government information systems to mock their security measures (Wikipedia, 2014c).</td>
<td>2011</td>
</tr>
<tr>
<td>Cutting Sword of Justice</td>
<td>Believed to be an Arab hacker group whose primary targets are the information technology resources of the Saudi government (Higgins, 2012).</td>
<td>2012</td>
</tr>
<tr>
<td>pHC</td>
<td>Pakistani based hacker group that conducts periodic defacements of Pakistani corporate and government websites (The Hacker's Post, 2013)</td>
<td>2013</td>
</tr>
<tr>
<td>Anonymous</td>
<td>International hacktivist collective that is increasingly focused on targeting information technology resources of government entities (Anonymous, 2013; Wikipedia, 2014a).</td>
<td>2004-Present</td>
</tr>
<tr>
<td>People’s Liberation Front</td>
<td>Canadian based hacktivist collective affiliated with Anonymous that primarily provides technical expertise to support protestors in other nations (The People's Liberation Front, 2014).</td>
<td>2013-Present</td>
</tr>
<tr>
<td>Syrian Electronic Army</td>
<td>A Pro-Syrian hacker group that targets U.S. government websites and supports the Assad regime (Bacon, 2013; Dugdale, 2014; Mendoza, 2013).</td>
<td>2013-Present</td>
</tr>
<tr>
<td>Redhack</td>
<td>Turkish based hacktivist collective whose primary targets are Turkish government information systems (Anonymous, A Brief History of Anonymous Hacktivism, 2013).</td>
<td>2013-Present</td>
</tr>
</tbody>
</table>

Note. From Anonymous, 2013; Anonymous, A Brief History of Anonymous Hacktivism, 2013; Bacon, 2013; Cult of the Dead Cow, 2014; Dugdale, 2014; Giest, 2014; Goodin & Dan, 2008;
Emerging Warning Problem

Earlier sections of the study provided an analysis and synthesis of the trends of hacktivist activities. This portion of the study includes an examination of the hacktivist activities that are emerging as warning signs of impending campaigns to attack the U.S. government to coerce government policy. Also, it provides an assessment of the probability and potential impacts of more radicalized hacktivist activity. This section includes an analysis of the emerging warning signs and of an anomaly from a broad field of information to provide scenarios from a range of plausible possibilities of the trajectory of hacktivist activities. There are five steps involved to predict future hacktivist activity:

1. Assess the cone of plausibility.
2. Sort out which scenarios to explore.
3. Determine if there is a warning message in any of the scenarios.
4. Identify or review.
5. Explore the opportunities.

This chapter covers Steps 1 and 2. The conclusion and analysis chapter of the study will include a discussion of the final three steps.
Environmental Scanning

As noted in the literature review, there are two common frameworks in use to conduct environmental scanning: PMESII-PT and STEMPLES. Because of the nature of cyberspace, not all of the factors in both frameworks are applicable. This study includes the common factors found in both frameworks that are applicable to the domain of cyberspace, politics, and socialization. The following sections are political and social environmental scans of the hacktivist community during 2014. The findings from the scans support the plausibility of the scenario that hacktivist activity contains the warning signs that it is becoming an emerging problem.
Table 4. Environment Scanning Factors.

<table>
<thead>
<tr>
<th>Environmental Scanning Factors</th>
<th>Descriptive Indicator 1 (DI1)</th>
<th>Descriptive Indicator 2 (DI2)</th>
<th>Descriptive Indicator 3 (DI3)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Political (P)</td>
<td>Encouragement of political activism (PDI1).</td>
<td>Claiming responsibility for cyberattacks (PDI2).</td>
<td>Threatened actions against legislators, governments, government officials, and those associated and affiliated with them (PDI3).</td>
</tr>
<tr>
<td>Social (S)</td>
<td>Promotion of protection of hacker community values (freedom of information and freedom of persecution from corporations and governments). Commentary. Praise of hacker actions (e.g., Snowden’s release of government documents) (SDI1).</td>
<td>Discussion/sharing of information to facilitate attacks. Discussion of new attack vectors and new exploits. Sharing of counterintelligence information, legal loopholes, and police and law enforcement operations (SDI2).</td>
<td>Discussion of future targets. Discussion of planned protest gatherings (SDI3).</td>
</tr>
</tbody>
</table>

*Note. Source: author.*

The first factor is the political factor. Hacktivist organizations are political activist organizations; thus, political drivers are the most important and influential factors to consider when assessing the radicalization of a group. Collectives of online personas where individuals congregate and socialize virtually with one another online comprise hacktivist organizations. This study examines the potential parallels among traditional activist organizations, such as the ELF and the ALF, which have had their members radicalized from their in-person interactions, and terrorist organizations. The social factor is the second factor to examine as an indicator of online radicalization of hacktivists who rely on cyberspace for their social interaction. Communication among fellow Anons (members of Anonymous) regarding discourse of the next issue they decide to intervene in and the selection of targets are descriptive indicators of hacktivist radicalization.
Political Environmental Scans

**Syrian Electronic Army (SEA) Hacks CNN website.** In January 2014, the Syrian Electronic Army (SEA) hacked news and social media accounts, including CNN, posting the following messages on CNN’s Twitter feed:

“So Syrian Electronic Army Was Here? Stop lying? All your reports are fake!?”

“DON’T FORGET: Al Qaeda is AL CIA da. Funded, armed and controlled.”

CNN responded by saying, “Some of our organization’s social media accounts were compromised. We have secured those accounts and are working to remedy the issue” (Department of Homeland Security, 2014, p. 1).

**Anonymous Announces OpPhDPounds.** In January 2014, Anonymous announced an operation code-named OpPhDPounds that would target government supported academic institutions. The campaign’s focus is to target academic institutions that have enrolled PhD students who are conducting research on Anonymous.

**Anonymous Claims to Have Hacked FBI.** In February 2014, a hacktivist group calling themselves the Black-Shadow, a Slovenian branch of Anonymous, claimed it had collaborated with AntiSec and LulzDec to hack the FBI and post email addresses and the director of the FBI’s personal information on Pastebin. Reportedly, Anonymous Slovenia posted the Pastebin link on its Facebook page with the comment “Laughing at your security” (PDI2) (Department of Homeland Security, 2014).

**Redhack Hack and Release of Turkish Government Officials.** In February 2014, Redhack released the names of hundreds of Turkish officials (PDI2) (Gilbert, 2014, p. xx).
**SEA Leaks Microsoft Invoices Sent to FBI.** In March 2014, the SEA leaked copies of Microsoft invoices from December 2012, August 2013, and November 2013, that showed the amount charged for each user’s data usage to the FBI’s Digital Intercept Technology Unit (DITU) to expose the corporation’s practice of selling information to the U.S. government (PDI2) (Department of Homeland Security, 2014).

**SEA Threatens U.S. Government.** In March 2014, the SEA threatened the U.S. government stating that if it conducted cyberattacks on the Assad regime, SEA would retaliate and show “that the entire U.S. command structure was a house of cards from the start” (PDI3) (Department of Homeland Security, 2014).

**SEA Targets United States Central Command (CENTCOM).** In March 2014, the SEA claimed to have compromised the systems of the United States Central Command (CENTCOM) in response to the U.S.’s intention to conduct cyber-warfare against Syria. The hackers claimed to have access to the Army Knowledge Online (AKO) and published a screenshot to demonstrate proof. According to the pro-Assad hacktivists, in the upcoming days, they will publish more data that will demonstrate the breach is more serious than it appears to be (PDI2) (PDI3) (Department of Homeland Security, 2014).

**Anonymous Declares Cyber-War on Countries Interfering With Ukraine.** In March 2014, Anonymous released a video declaring cyber-war on nations that pose a threat to Ukraine. In the video, the group warned the United States and NATO to refrain from involving themselves in Ukraine’s internal affairs. The video ended with the hackers stating, “We will strike at the Web resources of countries and organizations that pose a threat to freedom and independence of Ukraine!” (PDI3) (Department of Homeland Security, 2014).
**Anonymous Leaks Millions of Credit Cards.** In March 2014, members of the Anonymous hacking group based in Ukraine posted more than 7 million credit card numbers on the online storage website, Pastebin. The hackers claimed to have obtained information from more than 800 million cards, and this is reportedly only the first of other planned ‘data dumps.’ The majority of the credit card information released is from banks based in the United States (Department of Homeland Security, 2014).

Members of the Anonymous group posted a message stating, “After the USA showed its true face when she unilaterally decides which of the peoples to live independently and who under the yoke of the Federal Reserve, we decided to show the world who is behind the future collapse of the American banking system” (PDI2) (Department of Homeland Security, 2014).

**OpIsrael Launched by Anonymous and AnonGhost.** Members of the Anonymous and AnonGhost hacking groups launched OpIsrael on April 7, 2014, to protest Israel’s policies, including those concerning Palestine. During this operation, the groups defaced several small Israeli business websites. The groups also targeted the websites of Israeli ministries and organizations, threatening them with DDoS attacks (PDI2) (PDI3) (Department of Homeland Security, 2014).

**Tunisian Hacker Team Threatens United States.** In April 2014, Tunisian hackers posted a video online threatening to conduct cyberattacks on targets within the United States in a campaign they refer to as TheWeekOfHorror. The group has threatened to attack if the U.S. government does not remove its military forces from ‘Muhammad lands.’ The focus of TheWeekOfHorror, according to the group, would be the U.S. financial industry and airport computer systems (PDI3) (Department of Homeland Security, 2014).
Anonymous Hack and Release of Brazilian Military Police Employees. In May 2014, Anonymous hacked and released the identities of 181 people who were claimed to be Brazilian military police employees and shared the names, ranks, and phone numbers of the employees in this hack and release operation (PDI2) (Wagas, 2014).


Operation World Cup. In June 2014, Anonymous defaced Brazilian websites, including Brazil’s World Cup 2013 and Hyundai’s FIFA World Cup Soccer websites. The operation, dubbed Operation World Cup, was a protest against the state of domestic issues in Brazil (PDI2) (Symantec, 2014).

Protesting the Cyber Security Information Sharing Act (CISA). In July 2014, Anonymous threatened to conduct attacks against members of U.S. Congress and their families over the Cybersecurity Information Sharing Act of 2014 (CISA) (PDI3) (Cameron, 2014). Figures 8 through 11 show YouTube video postings of Anonymous protesting CISA.
Figure 8. Anonymous YouTube Video Protesting CISA. This is an illustration of a common symbol used to represent the hacktivist organization Anonymous. Adapted from Anonymous. (2014, July 30). #OpCISA. Retrieved from RT: rt.com/usa/169888-anonymous-cybersecurity-bil-wrath.
Figure 10. Anonymous YouTube Video Protesting CISA. Anonymous members are assembling in public to protest CISA. Adapted from Anonymous. (2014, July 30). #OpCISA. Retrieved from RT: rt.com/usa/169888-anonymous-cybersecurity-bil-wrath.
Operation Save Gaza. In protest of Israel’s incursion into Gaza and in retaliation for the death of one of its members at the hands of the Israeli Defense Forces, Anonymous launched Operation Save Gaza and hacked into several Israeli government departments, including the Israeli intelligence agency, Mossad, taking down the agency’s website for more than 10 hours with a DDoS attack. As part of Operation Save Gaza, Anonymous has targeted a number of other
Israeli organizations since July 7, 2014, defacing hundreds of Israeli government sites (PDI2) (Wei, 2014).

**City of Ferguson.** In August 2014, Anonymous claimed responsibility to hacking the City of Ferguson, Missouri in retaliation for police officer shooting an unarmed teenager (PDI2) (Baumer & McDonald, 2014).

**The First Reported Indication of Radicalization of a Hacktivist Collective.**

During Operation Save Gaza in August 2014, a campaign affiliated with Anonymous involving the attack of Israeli government websites in protest to Israeli actions in Gaza (Israel Operation Protective Edge), there are reports that members of the Anonymous collective were being infiltrated by the terrorist organization Hamas and other pro-terrorist organizations and their sympathizers (Cohen & Levin, 2014). This is the first reported indication that members of a hacktivist collective obtaining radicalized members that may push a more aggressive agenda to implement political change.
Figure 12. Protest Against Government Surveillance. This figure illustrates the encouragement of political activism (PDI1). Adapted from Anonymous (2014, August 1)
Figure 14. Promotion of Hacktivism. This figure illustrates the encouragement of political activism (PDII). Adapted from Anonymous (2014August 1) Anonymous. Retrieved from Twitter: www.twitter.com.
Social Environmental Scans

Figures 8 through 27 in Appendix B are scans of social media that include Facebook, Twitter, 4chan, and other hacker websites and blogs that show the current political atmosphere of hacktivist collectives.

Sort Out Which Scenarios to Explore

Scenario 1—Baseline

This scenario assumes that history will repeat itself and hacktivist groups will continue with their current tactics of website defacement, DDoS attacks, and hack and release measures to protest government and corporate practices they deem reprehensible.

Scenario 2—Plausible

Based on examinations of the ranked factors in Step 1 on page 86, this scenario identifies the more plausible development that hacktivists will intensify their focus on government targets, as shown in Chapter 2. Furthermore, it is plausible that hacktivists will adopt property destruction as a legitimate, nonviolent tactic as their traditional activist organizations’ predecessors, such as the ELF and ALF, have done. In this scenario, hacktivists would have to further radicalize and resort to property destruction as a means to make the costs of engaging in reprehensible practices large enough for the offenders that the hacktivists will receive a viable return on their investments and be successful in coercing governments and corporations into ceasing their contested practices. By resorting to property damage, the hacktivists become violent and terroristic in nature, evolving into cyberterrorists in parallel with ELF and ALF activists, who became terrorists when their members turned to property destruction to coerce governments and corporations.
Scenario 3—Wildcard

This scenario assumes a wildcard: that members of hacktivist organizations will radicalize online to the point where they may potentially resort to cyberattacks that could threaten the loss of life. This scenario is a wildcard because it is unlikely that such groups would intentionally attempt to commit acts that would cause the loss of lives. The ELF and ALF, though they have caused extensive property damage, took efforts to ensure that they did not kill anyone. Though acts of the ELF and ALF can be reckless and could accidentally cause loss of life if they are careless, it is unlikely that groups would plan intentionally deadly actions because any hacktivist campaign that would cause or support the loss of life would likely fail to garner support from the hacktivist community.
Chapter 5: Analysis and Conclusion

The analysis and conclusion section covers Steps 3 through 5 of the emerging warning problem regarding the threat hacktivist collectives pose to U.S. government agencies.

Determine if There is a Warning Message in any of the Scenarios

The first scenario (baseline) only considers the traditional hacktivist attacks of limited Distributed Denial of Service Attacks (DDoS) against government websites. These include typical hack and release operations of government employee personal information, hijacking of social media, and website defacement. None of these traditional attacks would warrant a warning message. Such attacks have not caused significant economic damage or threatened (or caused) loss of human life, thus crossing the threshold to becoming terrorist acts. However, a warning message is warranted in Scenarios 2 and 3 (plausible and wildcard), respectively. Scenario 2 is the more likely. There are already indicators of hacktivist organizations radicalizing and morphing their strategies parallel to the evolution of their environmental and animal rights activist cousins, and will resort to property destruction as tactic. If such a scenario were to occur, an attack or campaign against the information technology resources of U.S. government agencies is likely or imminent and warning is necessary to give government agencies sufficient lead-time to defend against these more serious threats. Scenario 3 is very unlikely, as hacktivist organizations have not yet been able to demonstrate the technological sophistication, or motivation, to cause loss of life.

Identify or Review

Within the next few years, it is unlikely that Scenario 3 will occur, though Scenario 2 is likely. The literature review identified calls within the hacker community for attacks on the U.S.
government. The case studies examined in Chapter 1 identify the potential impact cyber-attacks can have on a nation state. Chapter 2 identifies the trend of hacktivist attacks targeting government entities. Chapter 3 provides examples of recent calls in the hacktivist community for attacks on the U.S. government and its claims of responsibility for attacks that could potentially cause financial devastation (using information from millions of credit cards they obtained) along with the discussion among the community to consider attacking the U.S. financial sector (Wall Street). Furthermore, the calls within the hacktivist community in hacker publications, social media, and blogs to attack the U.S. government for its policies and operations are indicators that hacktivist groups may be evolving their strategies to cause economic damage in order to coerce the U.S. government to their whim. There are also recent indicators of radical members infiltrating hacktivist collectives. The conditions and drivers necessary for Scenario 2 to occur, and currently developing, are:

1. The U.S. increases its dependence on cyberspace to facilitate its instruments of national power according to the Diplomatic, Information, Military, and Economic (DIME) paradigm and cyberspace remains a U.S. strategic center of gravity.

2. Hacktivist trends continue to focus on selecting government targets with the intent to coerce nation-states to adopt actions the collective organizations desire. Members within the collective continue to call for attacks on the U.S. government.

3. Members within hacktivist collectives continue to congregate, socialize, and radicalize virtually.

4. Radicalized members within hacktivist collectives adopt strategies that parallel the evolution of environmental and animal rights activists and conduct attacks designed to cause
property damage to make whatever practice or policy they deem reprehensible too costly for the government to continue.

5. Banks and government entities fail to keep pace with hacktivist attack vectors to successfully defend against the same DDoS attacks that impacted American Express, Bank of America, JP Morgan Chase, Wells Fargo, U.S. Bank, and PNC Bank in 2013.

Explore Opportunities

Provided sufficient warning, several opportunities are present to thwart hacktivist attempts to attack government targets as part of a campaign to coerce the politics of the nation. One opportunity could be to implant informants or turn current members into informants in order to keep law enforcement appraised of hacktivist activities. This tactic was instrumental in dismantling LulzSec.

Another opportunity that exists to protect government systems from hacktivist campaigns could be to empower the Department of Homeland Security (DHS) with authorities over the .gov domain similar with those that United States Cyber Command (USCYBERCOM) currently possesses in governing and directing the defense of the .mil domain. USCYBERCOM possesses authorities to mitigate the types of attacks hacktivists have traditionally employed, such as DDoS attacks that could affect Department of Defense (DoD) missions. To protect DoD information technology resources from DDoS campaigns, USCYBERCOM can allocate sufficient bandwidth to DoD entities targeted to ensure they can withstand DDoS attacks. USCYBERCOM can also mandate Geo-blocking\(^4\) for all DoD entities to block traffic coming from predominately malicious IP addresses, direct the use of cloud-based services, reverse proxies for those targeted entities, and order minimum security postures based on threat indicators. DHS currently serves in

---

\(^4\) Geo-blocking is blocking access or content based on geographic location by excluding targeted Internet addresses.
an advisory capacity to federal agencies and does not possess these authorities. Based on the evidence in the study, it is likely that hacktivist collectives will target U.S. government agencies to coerce the U.S. government. If DHS were to receive these additional authorities, it would be empowered to direct the defense of the .gov domain to mitigate threats posed by hacktivists so that government agencies can continue to perform their missions.

Table 5. Answers to Research Questions.

<table>
<thead>
<tr>
<th>Research Questions</th>
<th>Answers</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Hacktivist motivations to conduct cyber-attacks.</td>
<td>Hacktivists motivations to conduct cyber-attacks include Internet Vigilantism, Victimizing, Deterrence, and Coercion against individuals, private organizations, corporate bodies, and government entities that engage in, or promote behavior that the collective finds reprehensible or threatening to their core values of transparency and freedom of information.</td>
</tr>
<tr>
<td>2. Trends and patterns of hacktivist targets and attacks.</td>
<td>Initially targeting primarily social groups, and then corporations, government entities are now the primary targets of hacktivist collectives.</td>
</tr>
<tr>
<td>3. Possible online radicalization of hacktivists in a virtual environment.</td>
<td>Virtual environments are the primary social environments and outlets for hacktivists. Hacktivist members can radicalize from their online interaction with like-minded individuals in collectives calling extreme action against targeted entities.</td>
</tr>
<tr>
<td>4. Indicators of online radicalization.</td>
<td>Indicators of online radicalization include increased frequency of calls for, and promotion of, attacks individuals, private organizations, corporate bodies, and government entities to deter, victimize, or coerce those targeted entities to influence their behavior and policies.</td>
</tr>
<tr>
<td>5. The reasons why hacktivists have yet to resort to acts of cyber terrorism.</td>
<td>Hacktivists have yet to resort to acts of cyber terrorism that could threaten the loss of life due to that action contradicting the collective’s core values. Hacktivists are an offshoot of Environmental and Animal Rights activists that took great care to avoid the loss of life in adopting property destruction as a tactic to coerce corporate and government entities.</td>
</tr>
</tbody>
</table>
Table 5. (continued)

<table>
<thead>
<tr>
<th>No.</th>
<th>Description</th>
<th>Considerations</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.</td>
<td>The likelihood that radicalized hacktivists will resort to acts of cyber</td>
<td>Property destruction is an act of violence. Groups that engage in property</td>
</tr>
<tr>
<td></td>
<td>terrorism.</td>
<td>destruction, such as the ELF and ALF, are terrorists. It is likely that</td>
</tr>
<tr>
<td></td>
<td></td>
<td>hacktivists will adopt property destruction as a tactic (along the same</td>
</tr>
<tr>
<td></td>
<td></td>
<td>evolutionary lines as Environmental and Animal Rights activist organizations</td>
</tr>
<tr>
<td></td>
<td></td>
<td>such as the ELF and ALF) and therefore resort to acts of cyber terrorism.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Furthermore, there are indicators that members, already radicalized, are</td>
</tr>
<tr>
<td></td>
<td></td>
<td>joining hacktivist groups, specifically the infiltration of Anonymous by</td>
</tr>
<tr>
<td></td>
<td></td>
<td>members of Hamas and other pro-terrorist organizations that may push for a</td>
</tr>
<tr>
<td></td>
<td></td>
<td>more aggressive agenda, such as acts of cyber terrorism, to implement political</td>
</tr>
<tr>
<td></td>
<td></td>
<td>change (Cohen &amp; Levin, 2014).</td>
</tr>
<tr>
<td>7.</td>
<td>Explore the value of developing an emerging warning regarding the potential</td>
<td>An emerging warning problem would support the warning mission of the U.S.</td>
</tr>
<tr>
<td></td>
<td>threat of radicalized hacktivists conducting cyber terror attacks to further</td>
<td>Intelligence Community and enable the posturing of government resources to</td>
</tr>
<tr>
<td></td>
<td>political agendas.</td>
<td>prevent acts and or mitigate acts of cyber terrorism and their effects.</td>
</tr>
</tbody>
</table>

*Note.* Source: author.

**Recommendations**

The researcher recommends that the Intelligence Community publish the following emerging warning problem to the Defense Warning Network.

**Radicalization of Hacktivist Collectives Will Seek to Impede DOD Operations**

**Nature of the Threat.** Hacktivists are an offshoot of environment and animal rights groups such as the ELF and the ALF, both of which have adopted a strategy of property destruction as a means to coerce corporations and government to end practices they despise by making those practices too costly to continue. The Federal Bureau of Investigation classifies the ELF and ALF as terrorist organizations (Jarboe, 2002). Since 2010, there is an increasing trend of hacktivist organizations targeting government entities and that these groups are beginning to radicalize. It is likely that there will be hacktivist organizations that radicalize and resort to acts of cyber sabotage to impede DOD operations.
The April 2014 edition of the hacker magazine 2600 published a subscriber’s letter calling for an attack by the collective community of hackers on the NSA to thwart its collection activities. Instead of advising against such an action as it has in response to previous letters expressing similar sentiments, the editorial staff was silent on the issue and instead offered advice on how users can remain anonymous if engaged in risky, illegal behavior online (justanothersubscriber, 2014).

According to the U.S. Department of Homeland Security, Middle Eastern and North African hackers, acting in the name of Anonymous, made preparations to conduct cyber-attacks against the websites of high-profile U.S. government agencies, banks, and other companies in an operation they called #OpUSA in May 2013. There was an announcement on the electronic bulletin board Pastebin calling for the operation to begin on Tuesday, May 7, 2013 (Waterman, 2013). The attacks planned for May 7 were, however, a failure: no high-profile sites were taken offline, and only a few lesser sites were compromised and defaced (Huang, 2013).

In August 2014, during Anonymous Operation Save Gaza, there were reports that members of the Anonymous collective were being infiltrated by the terrorist organization Hamas and other pro-terrorist organizations and their sympathizers (Cohen & Levin, 2014). This is the first reported indication that members of a hacktivist collective obtaining radicalized members that may push a more aggressive agenda to implement political change.

As shown in Figure 15, hacktivist collectives are beginning to radicalize and will continue to focus on targeting government entities which include DOD assets. As with Operation Save Gaza, hacktivist collectives will radicalize and will seek to impede or hinder DOD operations in protest to U.S. military involvement.
Figure 15. Trends of Hacktivist Attacks. Hacktivists are increasingly targeting government entities.
**Implications.** The implications of a hacktivist campaign designed to disrupt DOD operations can be a denial of service attack on the DOD unclassified networks, or the unclassified networks of coalition partners and commercial vendors.

**Warning Posture.** There are some key differences between hacktivists and profiteering hackers. Though both do develop some custom built applications, both typically rely on inexpensive, off-the-shelf tools to conduct attacks. Both also tend not to use botnets or rely upon malware, unlike for-profit hackers, nor do they often develop phishing or spear phishing emails. Lastly, a key difference between hacktivists and profiteering hackers is their method of recruitment. Profiteering hackers tend to recruit members in private hacker forum, whereas, hacktivists recruit openly in social media outlets (Imperva, 2012). Hacktivists’ reliance on open communication methods allow for the monitoring of their activity and intended targets.

**Conditions and Drivers.**

1. Hacktivist trends continue to focus on selecting government targets with the intent to coercing nation-states to adopt actions the collective organizations desire. Members within the collective continue to call for attacks on the U.S. government.

2. Members within hacktivist collectives continue to congregate, socialize, and radicalize virtually.

3. Radicalized members within hacktivist collectives adopt strategies that parallel the evolution of environmental and animal rights activists and conduct attacks designed to cause property damage to make whatever practice or policy they deem reprehensible too costly for the government to continue.
**Key Indicators.** Hacktivists typically employ the same hacking methods that profiteering hackers use and will often try to steal data first before resorting to more brute force measures such as a Distributed Denial of Service (DDoS) attack. There are two types of members within a hacktivist collective: skilled hackers and laypeople. The skilled hacker group is the more dangerous, they are capable of writing their own code and tools and display genuine hacking skills. Typically, a hacktivist collective has no more than 10 to 15 individuals who are skilled hackers. The second group, laypeople (also known as ‘script kiddies’), are individuals with few skills who can use automated hacking tools with little to no training. The number of people in this group can be quite large, ranging from anywhere from a few dozen, to a few hundred (Imperva, 2012).

Hacking operations fall into three phases:

1. **Phase 1: Recruiting and communications phase.** In this phase, hacktivists frequently leverage social media to recruit members, promote their campaign, and justify attacking the targets selected.

2. **Phase 2: Reconnaissance and application attack phase.** In the second phase, hacktivists will attempt to mask their identity and base of operations as they probe target applications to identify weaknesses that could result in a data breach.

3. **Phase 3: DDoS phase.** If a data breach fails, the skilled hackers group will often elicit help from laypeople, who, in large numbers, will download attack software to conduct more destructive actions, such as a DDoS attack.
Opportunities to Influence. Monitoring of hacker and hacktivist chat rooms, blogs, publications, and websites can provide situational awareness of impending hacktivist attacks on DOD networks.

Conclusion

The results of the study indicate that members of hacktivists collectives rely upon cyberspace as their primary medium for social interaction. There are indications that these groups are seeking to challenge government authority within cyberspace and are increasingly targeting government entities. There are also indications that through their social interactions in cyberspace that they are beginning to radicalize and will seek to coerce nations and military operations by attacking targets in cyberspace, viewing property destruction as a legitimate strategy to obtain their objectives. The IC will need to codify a warning problem to give decision-makers adequate response time to mitigate this new threat.
References


www.youtube.com/watch?v=mtl4sxzIVoA


http://d26e8pvoto2x3r.cloudfront.net/uploadimages/Import/(FILE)1333533336.pdf


http://www.wired.com/2012/07/ff_anonymous/all/


http://bits.blogs.nytimes.com/2012/09/27/hackers-may-have-had-help-with-attacks-on-u-s-banks-researchers-say/?_php=true&_type=blogs&_r=0


Wikipedia. (2014a, October 5). *Anonymous (group)*. Retrieved from Wikipedia:
http://en.wikipedia.org/wiki/Anonymous_(group)

http://en.wikipedia.org/wiki/Cult_of_the_Dead_Cow

http://en.wikipedia.org/wiki/Lulzsec


http://terrorism.about.com/od/groupsleader1/p/Sicarii.htm

www.facebook.com/AnonymousOperations
### Appendix A: Data on Hacktivist Collectives

Table 6. Cult of the Dead Cow.

<table>
<thead>
<tr>
<th>Year(s)</th>
<th>Target/Operation</th>
<th>Description</th>
<th>Action</th>
<th>Sector</th>
<th>Objective/Motivation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1990s</td>
<td>Hong Kong Blondes</td>
<td>Disrupted People’s Republic of China (PRC) networks to allow PRC citizens to access censored content online</td>
<td>Support</td>
<td>Government</td>
<td>Internet Vigilantism</td>
</tr>
<tr>
<td>1999</td>
<td>Cyber war</td>
<td>Joined a loose coalition of hacker to denounce a call to cyber war against the governments of China and Iraq</td>
<td>Social Justice</td>
<td>Government</td>
<td>Deterrence</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Social Justice</td>
<td>Social Group</td>
<td>Deterrence</td>
</tr>
<tr>
<td>2002</td>
<td>Milosevic trial</td>
<td>Published questioning of Dr. Patrick Ball</td>
<td>Social Justice</td>
<td>Social Group</td>
<td>Internet Vigilantism</td>
</tr>
<tr>
<td>2002</td>
<td>Goolag campaign</td>
<td>Hacktivist publications criticizing Microsoft, Yahoo, Google, and CISCO decision to comply with PRC internet policies</td>
<td>Social Justice</td>
<td>Corporate</td>
<td>Deterrence</td>
</tr>
</tbody>
</table>

*Note.* From *Cult of the Dead Cow*. Retrieved from Wikipedia

Table 7. Syrian Electronic Army.

<table>
<thead>
<tr>
<th>Year(s)</th>
<th>Target/Operation</th>
<th>Description</th>
<th>Action</th>
<th>Sector</th>
<th>Objective/Motivation</th>
</tr>
</thead>
<tbody>
<tr>
<td>2013</td>
<td>White House Staffers</td>
<td>Compromise of White House staffers personal email accounts</td>
<td>Harassment</td>
<td>Government</td>
<td>Coercion</td>
</tr>
<tr>
<td>2013</td>
<td>NY Times takedown; Twitter problems</td>
<td>DDoS Attack on NY Times website and Twitter</td>
<td>Harassment</td>
<td>Government</td>
<td>Coercion</td>
</tr>
<tr>
<td>2013</td>
<td>U.S. Marines website</td>
<td>Website defacement</td>
<td>Retaliation</td>
<td>Government</td>
<td>Coercion</td>
</tr>
</tbody>
</table>

*Note.* From Bacon, 2013; Dugdale 2014; Mendoza, 2013.
Table 8. pHC, a Hacktivist Organization.

**Timeline**

<table>
<thead>
<tr>
<th>Year(s)</th>
<th>Target/Operation</th>
<th>Description</th>
<th>Action</th>
<th>Sector</th>
<th>Objective/Motivation</th>
</tr>
</thead>
<tbody>
<tr>
<td>2008</td>
<td>StillSecure</td>
<td>Ransacking security researcher accounts, redirecting web traffic</td>
<td>Harassment</td>
<td>Corporate</td>
<td>Victimization</td>
</tr>
<tr>
<td>2008</td>
<td>Kevin Mitnick</td>
<td>Ransacking security researcher accounts, redirecting web traffic</td>
<td>Harassment</td>
<td>Private Person</td>
<td>Victimization</td>
</tr>
<tr>
<td>2008</td>
<td>Nate Lawson</td>
<td>Ransacking security researcher accounts, redirecting web traffic</td>
<td>Harassment</td>
<td>Private Person</td>
<td>Victimization</td>
</tr>
<tr>
<td>2008</td>
<td>Pedtko D. Petkov</td>
<td>Ransacking security researcher accounts, redirecting web traffic</td>
<td>Harassment</td>
<td>Private Person</td>
<td>Victimization</td>
</tr>
<tr>
<td>2008</td>
<td>Tom Ferris</td>
<td>Ransacking security researcher accounts, redirecting web traffic</td>
<td>Harassment</td>
<td>Private Person</td>
<td>Victimization</td>
</tr>
<tr>
<td>2008</td>
<td>Thomas Ptacek</td>
<td>Ransacking security researcher accounts, redirecting web traffic</td>
<td>Harassment</td>
<td>Private Person</td>
<td>Victimization</td>
</tr>
<tr>
<td>2008</td>
<td>OWASP</td>
<td>Ransacking security researcher accounts, redirecting web traffic</td>
<td>Harassment</td>
<td>Corporate</td>
<td>Victimization</td>
</tr>
<tr>
<td>2008</td>
<td>Kurt Seifried</td>
<td>Ransacking security researcher accounts, redirecting web traffic</td>
<td>Harassment</td>
<td>Private Person</td>
<td>Victimization</td>
</tr>
<tr>
<td>2008</td>
<td>Alan Shimel</td>
<td>Ransacking security researcher accounts, redirecting web traffic</td>
<td>Harassment</td>
<td>Private Person</td>
<td>Victimization</td>
</tr>
<tr>
<td>2008</td>
<td>Security Bloggers Network</td>
<td>Ransacking security researcher accounts, redirecting web traffic</td>
<td>Harassment</td>
<td>Corporate</td>
<td>Victimization</td>
</tr>
<tr>
<td>2008</td>
<td>Core Security</td>
<td>Ransacking security researcher accounts, redirecting web traffic</td>
<td>Harassment</td>
<td>Corporate</td>
<td>Victimization</td>
</tr>
</tbody>
</table>

*Note. From Archives for Pakistan Haxors Crew. Retrieved from The Hacker’s Post:*

Table 9. giest, a Hacktivist Organization.

**Timeline**

<table>
<thead>
<tr>
<th>Year(s)</th>
<th>Target/Operation</th>
<th>Description</th>
<th>Action</th>
<th>Sector</th>
<th>Objective/Motivation</th>
</tr>
</thead>
<tbody>
<tr>
<td>2013</td>
<td>Geo News Website</td>
<td>Website</td>
<td>Harassment</td>
<td>Corporate</td>
<td>Victimization</td>
</tr>
<tr>
<td>2013</td>
<td>Election Commission of Nepal</td>
<td>Website defacement</td>
<td>Harassment</td>
<td>Corporate</td>
<td>Victimization</td>
</tr>
<tr>
<td>2013</td>
<td>Official NUST SEECS subdomain</td>
<td>Website defacement</td>
<td>Harassment</td>
<td>Corporate</td>
<td>Victimization</td>
</tr>
<tr>
<td>2013</td>
<td>Mobilink Careers</td>
<td>Website defacement</td>
<td>Harassment</td>
<td>Corporate</td>
<td>Victimization</td>
</tr>
<tr>
<td>2013</td>
<td>Innovation Punjab</td>
<td>Website defacement</td>
<td>Harassment</td>
<td>Government</td>
<td>Victimization</td>
</tr>
<tr>
<td>2013</td>
<td>Federally Administered Tribal Areas</td>
<td>Website defacement</td>
<td>Harassment</td>
<td>Government</td>
<td>Victimization</td>
</tr>
<tr>
<td></td>
<td>Government website</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2013</td>
<td>Cyber War: Pakistani Hacker retaliates,</td>
<td>Website defacements</td>
<td>Retaliation</td>
<td>Government</td>
<td>Coercion</td>
</tr>
<tr>
<td></td>
<td>hacks thousands of Indian websites</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Note. From giest, 2014; Goodin & Dan, 2008; Wikipedia, 2014a.*

Table 10. ~EL8, a Hacktivist Organization.

**Timeline**

<table>
<thead>
<tr>
<th>Year(s)</th>
<th>Target/Operation</th>
<th>Description</th>
<th>Action</th>
<th>Sector</th>
<th>Objective/Motivation</th>
</tr>
</thead>
<tbody>
<tr>
<td>2002</td>
<td>Project Mayhem</td>
<td>Targeted Security Professionals by spreading a Trojan</td>
<td>Harassment</td>
<td>Corporate</td>
<td>Victimization</td>
</tr>
</tbody>
</table>

Table 11. Naija Cyber Hacktivists.

**Timeline**

<table>
<thead>
<tr>
<th>Year(s)</th>
<th>Target/Operation</th>
<th>Description</th>
<th>Action</th>
<th>Sector</th>
<th>Objective/Motivation</th>
</tr>
</thead>
<tbody>
<tr>
<td>2011</td>
<td>napep.gov.ng</td>
<td>Targeting of Nigerian government website in protest to the organization's failure to do its stated purpose of helping poverty stricken children</td>
<td>Social Justice</td>
<td>Government</td>
<td>Coercion</td>
</tr>
<tr>
<td>2011</td>
<td>Operation FOI</td>
<td>Targeting Nigerian government websites to influence Nigerian President to sign a piece of legislation (Freedom of Information) into law</td>
<td>Harassment</td>
<td>Government</td>
<td>Coercion</td>
</tr>
<tr>
<td>2011</td>
<td>Operation Nigeria Black</td>
<td>Targeting of Nigerian government offices</td>
<td>Harassment</td>
<td>Government</td>
<td>Coercion</td>
</tr>
</tbody>
</table>

*Note. From The Story of Nigeria's First Cyber Hacktivists. Retrieved from Storify:*  
Table 12. The People’s Liberation Front.

**Timeline**

<table>
<thead>
<tr>
<th>Year(s)</th>
<th>Target/Operation</th>
<th>Description</th>
<th>Action</th>
<th>Sector</th>
<th>Objective/Motivation</th>
</tr>
</thead>
<tbody>
<tr>
<td>2011</td>
<td>Operation USA</td>
<td>Attack in protest to Oakland police brutality</td>
<td>Retaliation</td>
<td>Corporate</td>
<td>Coercion</td>
</tr>
<tr>
<td>2012</td>
<td>Operation Freedom Star</td>
<td>Acquisition of end of life low orbit satellites for use a covert communication channels</td>
<td>Support</td>
<td>Corporate</td>
<td>Deterrence</td>
</tr>
<tr>
<td>2012</td>
<td>Operation Anaheim</td>
<td>Call for Disneyland Boycott</td>
<td>Retaliation</td>
<td>Corporate</td>
<td>Coercion</td>
</tr>
<tr>
<td>2012</td>
<td>Operation TrapWire</td>
<td>Joined Anonymous in targeting of facial recognition software</td>
<td>Harassment</td>
<td>Government</td>
<td>Coercion</td>
</tr>
<tr>
<td>2012</td>
<td>Operation Syria</td>
<td>Joined Anonymous to support Syrian protestors</td>
<td>Support</td>
<td>Government</td>
<td>Coercion</td>
</tr>
<tr>
<td>2012</td>
<td>Operation Paraguay</td>
<td>Joined Anonymous to support Paraguay protestors</td>
<td>Support</td>
<td>Government</td>
<td>Coercion</td>
</tr>
<tr>
<td>2012</td>
<td>Operation Ethiopia</td>
<td>Joined Anonymous to support Ethiopian protestors</td>
<td>Support</td>
<td>Government</td>
<td>Coercion</td>
</tr>
<tr>
<td>2013</td>
<td>Operation Bahrain</td>
<td>Joined Anonymous to support Bahrain protestors</td>
<td>Support</td>
<td>Government</td>
<td>Coercion</td>
</tr>
</tbody>
</table>

*Note. From* Internet Freedom Fighters. Retrieved from Peoples Liberation Front:

http://www.plf.eu.pn.
Table 13. Cutting Sword of Justice.

**Timeline**

<table>
<thead>
<tr>
<th>Year(s)</th>
<th>Target/Operation</th>
<th>Description</th>
<th>Action</th>
<th>Sector</th>
<th>Objective/Motivation</th>
</tr>
</thead>
<tbody>
<tr>
<td>2012</td>
<td>Saudi Aramco workstations</td>
<td>Data destroying attack on Saudi oil company.</td>
<td>Harassment</td>
<td>Corporate</td>
<td>Victimization</td>
</tr>
</tbody>
</table>

Table 14. Thehacker12.

**Timeline**

<table>
<thead>
<tr>
<th>Year(s)</th>
<th>Target/Operation</th>
<th>Description</th>
<th>Action</th>
<th>Sector</th>
<th>Objective/Motivation</th>
</tr>
</thead>
<tbody>
<tr>
<td>2011</td>
<td>allianceforbiz.com</td>
<td>Released stolen data</td>
<td>Harassment</td>
<td>Corporate</td>
<td>Victimization</td>
</tr>
<tr>
<td>2011</td>
<td>Small Business Administration</td>
<td>Release of government employee personal information</td>
<td>Harassment</td>
<td>Government</td>
<td>Victimization</td>
</tr>
<tr>
<td>2011</td>
<td>musicbizpro</td>
<td>Release of site database</td>
<td>Harassment</td>
<td>Corporate</td>
<td>Victimization</td>
</tr>
<tr>
<td>2011</td>
<td>Kongu Polytechnic College</td>
<td>Exposure of corrupt college officials</td>
<td>Social justice</td>
<td>Social Group</td>
<td>Victimization</td>
</tr>
<tr>
<td>2011</td>
<td>Association of Cosmetic Laser Surgeons</td>
<td>Hacking of association website and release of association members' name and email addresses</td>
<td>Harassment</td>
<td>Social Group</td>
<td>Victimization</td>
</tr>
<tr>
<td>2011</td>
<td>Bulls</td>
<td>Hacking of Stock Broking company database</td>
<td>Harassment</td>
<td>Corporate</td>
<td>Victimization</td>
</tr>
<tr>
<td>2011</td>
<td>Maulana Azad Institute of dental college</td>
<td>Hacking of educational website</td>
<td>Social justice</td>
<td>Social Group</td>
<td>Victimization</td>
</tr>
<tr>
<td>2011</td>
<td>Chennai Traffic Police</td>
<td>Release of server and password information</td>
<td>Harassment</td>
<td>Government</td>
<td>Victimization</td>
</tr>
<tr>
<td>2011</td>
<td>Café coffee day</td>
<td>Release of company coupon database</td>
<td>Harassment</td>
<td>Corporate</td>
<td>Victimization</td>
</tr>
<tr>
<td>2011</td>
<td>Apnaby.in</td>
<td>Hacking of bus booking agency in India</td>
<td>Harassment</td>
<td>Corporate</td>
<td>Victimization</td>
</tr>
<tr>
<td>2011</td>
<td>saosaosao.com</td>
<td>Hacking of Thai girls band</td>
<td>Harassment</td>
<td>Corporate</td>
<td>Victimization</td>
</tr>
<tr>
<td>2011</td>
<td>Unlockitnow.com</td>
<td>Release of 10,000 account passwords</td>
<td>Harassment</td>
<td>Corporate</td>
<td>Victimization</td>
</tr>
<tr>
<td>2011</td>
<td>rycorealty.com</td>
<td>Release of admin passwords</td>
<td>Harassment</td>
<td>Corporate</td>
<td>Victimization</td>
</tr>
<tr>
<td>2011</td>
<td>Apniissp.com</td>
<td>South Asian music site hacked. Usernames and passwords released</td>
<td>Harassment</td>
<td>Corporate</td>
<td>Victimization</td>
</tr>
<tr>
<td>2011</td>
<td>VVTV (Italy)</td>
<td>Hacking of an Italian television website</td>
<td>Harassment</td>
<td>Corporate</td>
<td>Victimization</td>
</tr>
<tr>
<td>2011</td>
<td>Script World (Germany)</td>
<td>Release of company database</td>
<td>Harassment</td>
<td>Corporate</td>
<td>Victimization</td>
</tr>
<tr>
<td>2011</td>
<td>Pizza hut (India)</td>
<td>Release of admin username and password</td>
<td>Harassment</td>
<td>Corporate</td>
<td>Victimization</td>
</tr>
<tr>
<td>2011</td>
<td>Bharat Sanchar Nigam Ltd (BSNL) Network</td>
<td>Hacking of a Indian telecom company</td>
<td>Social justice</td>
<td>Corporate</td>
<td>Coercion</td>
</tr>
</tbody>
</table>
Table 14. (continued)

<table>
<thead>
<tr>
<th>Year</th>
<th>Target/Operation</th>
<th>Action</th>
<th>Sector</th>
<th>Objective/Motivation</th>
</tr>
</thead>
<tbody>
<tr>
<td>2011</td>
<td>English Football Club</td>
<td>Release of club database</td>
<td>Harassment</td>
<td>Corporate</td>
</tr>
<tr>
<td>2011</td>
<td>PCS Consultants</td>
<td>Release of company database</td>
<td>Harassment</td>
<td>Corporate</td>
</tr>
<tr>
<td>2011</td>
<td>Weebly</td>
<td>Identification of vulnerability</td>
<td>Harassment</td>
<td>Corporate</td>
</tr>
<tr>
<td>2011</td>
<td>Indian Oil</td>
<td>Identification of vulnerability</td>
<td>Harassment</td>
<td>Corporate</td>
</tr>
<tr>
<td>2011</td>
<td>funniestvideosonline.com</td>
<td>Release of 3,300 email addresses and passwords</td>
<td>Harassment</td>
<td>Corporate</td>
</tr>
<tr>
<td>2011</td>
<td>Wikipedia</td>
<td>Identification of vulnerability</td>
<td>Harassment</td>
<td>Corporate</td>
</tr>
<tr>
<td>2011</td>
<td>Camber</td>
<td>Release of admin information</td>
<td>Harassment</td>
<td>Corporate</td>
</tr>
<tr>
<td>2011</td>
<td>wrestlegame.co.uk</td>
<td>Release of database</td>
<td>Harassment</td>
<td>Corporate</td>
</tr>
</tbody>
</table>

Note. From (Thehacker12, 2014; Wikipedia, 2014).

Table 15. Antisec.

Timeline

<table>
<thead>
<tr>
<th>Year(s)</th>
<th>Target/Operation</th>
<th>Description</th>
<th>Action</th>
<th>Sector</th>
<th>Objective/Motivation</th>
</tr>
</thead>
<tbody>
<tr>
<td>2011</td>
<td>Pfizer</td>
<td>Hacked Facebook page of pharmaceutical company</td>
<td>Harassment</td>
<td>Corporate</td>
<td>Victimizing</td>
</tr>
<tr>
<td>2011</td>
<td>Redhack</td>
<td>Defacement of over 1000 websites in Turkey</td>
<td>Harassment</td>
<td>Government</td>
<td>Victimizing</td>
</tr>
<tr>
<td>2011</td>
<td>Tamil.Canadian.com</td>
<td>Publishing of usernames and passwords</td>
<td>Harassment</td>
<td>Social Group</td>
<td>Victimizing</td>
</tr>
<tr>
<td>2011</td>
<td>Stevens Institute Technology</td>
<td>Leaking of website database</td>
<td>Harassment</td>
<td>Corporate</td>
<td>Victimizing</td>
</tr>
<tr>
<td>2011</td>
<td>Pepper.nl and Nimbuzz</td>
<td>Hacked into websites</td>
<td>Harassment</td>
<td>Corporate</td>
<td>Victimizing</td>
</tr>
<tr>
<td>2011</td>
<td>House of Representatives of the Philippines</td>
<td>Posting personal information of members of Congress</td>
<td>Harassment</td>
<td>Government</td>
<td>Victimizing</td>
</tr>
</tbody>
</table>

Table 16. Lulzsec.

<table>
<thead>
<tr>
<th>Year(s)</th>
<th>Target/Operation</th>
<th>Description</th>
<th>Action</th>
<th>Sector</th>
<th>Objective/Motivation</th>
</tr>
</thead>
<tbody>
<tr>
<td>2011</td>
<td>Fox News</td>
<td>Leaked passwords, LinkedIn profiles and 73,000 X Factor contestants</td>
<td>Retaliation</td>
<td>Corporate</td>
<td>Victimizing</td>
</tr>
<tr>
<td>2011</td>
<td>ATM attack in Britain</td>
<td>Released transaction logs of 3,100 Automated Teller Machines in UK</td>
<td>Harassment</td>
<td>Corporate</td>
<td>Victimizing</td>
</tr>
<tr>
<td>2011</td>
<td>PBS Website</td>
<td>stole user data and posted fake stories</td>
<td>Harassment</td>
<td>Corporate</td>
<td>Victimizing</td>
</tr>
<tr>
<td>2011</td>
<td>Sony pictures</td>
<td>stole user data</td>
<td>Retaliation</td>
<td>Corporate</td>
<td>Deterrence</td>
</tr>
<tr>
<td>2011</td>
<td>Nintendo</td>
<td>Attempted attack</td>
<td>Support</td>
<td>Corporate</td>
<td>Coercion</td>
</tr>
<tr>
<td>2011</td>
<td><a href="http://www.pron.com">www.pron.com</a></td>
<td>stole and published user information</td>
<td>Harassment</td>
<td>Corporate</td>
<td>Victimizing</td>
</tr>
<tr>
<td>2011</td>
<td>Bethesda Game Studios</td>
<td>stole user data</td>
<td>Harassment</td>
<td>Corporate</td>
<td>Coercion</td>
</tr>
<tr>
<td>2011</td>
<td>MediaFrie</td>
<td>postings an assortment of passwords to the 4chan/b/board</td>
<td>Support</td>
<td>Social Group</td>
<td>Internet Vigilantism</td>
</tr>
<tr>
<td>2011</td>
<td>InfraGard</td>
<td>Hacked local chapter sites of a group affiliated with the FBI</td>
<td>Harassment</td>
<td>Social Group</td>
<td>Coercion</td>
</tr>
<tr>
<td>2011</td>
<td>British National Health Service</td>
<td>Discovery of security vulnerability</td>
<td>Support</td>
<td>Government</td>
<td>Coercion</td>
</tr>
<tr>
<td>2011</td>
<td>Senate.gov</td>
<td>released emails and passwords of users</td>
<td>Harassment</td>
<td>Government</td>
<td>Coercion</td>
</tr>
<tr>
<td>2011</td>
<td>Central Intelligence Agency</td>
<td>Attacked CIA website</td>
<td>Harassment</td>
<td>Government</td>
<td>Coercion</td>
</tr>
<tr>
<td>2011</td>
<td>Bank of Portugal, Assembly of the Republic, Ministry of Economy, and Innovation and Development</td>
<td>DDoS attacks on sites related to the government of Portugal</td>
<td>Harassment</td>
<td>Government</td>
<td>Coercion</td>
</tr>
</tbody>
</table>

Table 17. Redhack.

**Timeline**

<table>
<thead>
<tr>
<th>Year(s)</th>
<th>Target/Operation</th>
<th>Description</th>
<th>Action</th>
<th>Sector</th>
<th>Objective/Motivation</th>
</tr>
</thead>
<tbody>
<tr>
<td>2013</td>
<td>Turkey Minister to EU affairs</td>
<td>Leaking of 18 documents</td>
<td>Harassment</td>
<td>Government</td>
<td>Victimization</td>
</tr>
<tr>
<td>2013</td>
<td>Abdullah</td>
<td>Release of documents with the names of Turkish officers that killed Turkish</td>
<td>Harassment</td>
<td>Government</td>
<td>Internet Vigilantism</td>
</tr>
<tr>
<td></td>
<td></td>
<td>protestor 'Abdullah'</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2013</td>
<td>SECSiS</td>
<td>Computer Supported Central Voter Registry System threat.</td>
<td>Social Justice</td>
<td>Government</td>
<td>Coercion</td>
</tr>
<tr>
<td>2013</td>
<td>Turkish Police</td>
<td>Taking down police website.</td>
<td>Harassment</td>
<td>Government</td>
<td>Coercion</td>
</tr>
<tr>
<td>2013</td>
<td>Turkey's Directorate of Religious Affairs</td>
<td>Took down government website</td>
<td>Social Justice</td>
<td>Government</td>
<td>Internet Vigilantism</td>
</tr>
<tr>
<td>2013</td>
<td>Istanbul Special Provincial Administration</td>
<td>Release of documents</td>
<td>Harassment</td>
<td>Government</td>
<td>Coercion</td>
</tr>
<tr>
<td>2013</td>
<td>Police Department Website of Ankara</td>
<td>Website defacement</td>
<td>Harassment</td>
<td>Government</td>
<td>Coercion</td>
</tr>
<tr>
<td>2013</td>
<td>#OpTurkey</td>
<td>List of Turkish Government websites defaced</td>
<td>Harassment</td>
<td>Government</td>
<td>Coercion</td>
</tr>
<tr>
<td>2013</td>
<td>Reyhanli explosion</td>
<td>Release of secret military documents</td>
<td>Harassment</td>
<td>Government</td>
<td>Coercion</td>
</tr>
<tr>
<td>2013</td>
<td>Turkish officials</td>
<td>Leaking details of hundreds of Turkish officials</td>
<td>Harassment</td>
<td>Government</td>
<td>Victimization</td>
</tr>
</tbody>
</table>

Table 18. Anonymous.

<table>
<thead>
<tr>
<th>Year(s)</th>
<th>Target/Operation</th>
<th>Description</th>
<th>Action</th>
<th>Sector</th>
<th>Objective/Motivation</th>
</tr>
</thead>
<tbody>
<tr>
<td>2004</td>
<td>Encyclopedia Dramatica</td>
<td>Online meeting place for Anons. Serves as a forum for online documentation of Anonymous gossip. The site is filled with misogynist and racism rhetoric</td>
<td>Support</td>
<td>Social group</td>
<td>Victimizing</td>
</tr>
<tr>
<td>2006-2007</td>
<td>Habbo</td>
<td>Social networking site, where moderators had a tendency to ban users based on the skin colors of their avatars</td>
<td>Harassment</td>
<td>Corporate</td>
<td>Internet Vigilantism</td>
</tr>
<tr>
<td>2006-2007</td>
<td>Hal Turner</td>
<td>Controversial business - Radio Talk Show, White Supremacist</td>
<td>Harassment</td>
<td>Corporate</td>
<td>Internet Vigilantism</td>
</tr>
<tr>
<td>2006-2007</td>
<td>Chris Forecand</td>
<td>Arrest of a pedophile, in Toronto Canada as a result of internet vigilantism</td>
<td>Harassment</td>
<td>Private Person</td>
<td>Internet Vigilantism</td>
</tr>
<tr>
<td>2008</td>
<td>Church of Scientology</td>
<td>Church sought to censor the release of an unauthorized video.</td>
<td>Harassment</td>
<td>Religious Entity</td>
<td>Internet Vigilantism</td>
</tr>
<tr>
<td>2008</td>
<td>Epilepsy Foundation</td>
<td>Anonymous uses posting JavaScript code and flashing animations in an attempt to cause migraines and epileptic seizures for members of an epilepsy support forum.</td>
<td>Harassment</td>
<td>Social group</td>
<td>Victimizing</td>
</tr>
<tr>
<td>2008</td>
<td>SOHH and AllHipHop</td>
<td>Retaliation for being insulted by members of SOHH social community</td>
<td>Retaliation</td>
<td>Social group</td>
<td>Deterrence</td>
</tr>
<tr>
<td>2008</td>
<td>Sarah Palin</td>
<td>Hacking Sarah Palin's email account</td>
<td>Harassment</td>
<td>Government</td>
<td>Victimizing</td>
</tr>
<tr>
<td>2009</td>
<td>No Cussing Club</td>
<td>Targeted teenager that hosted a website against profanity</td>
<td>Harassment</td>
<td>Private Person</td>
<td>Victimizing</td>
</tr>
<tr>
<td>2009</td>
<td>Iranian election</td>
<td>Launched websites to circumvent Iranian censorship during 2009 Iranian elections</td>
<td>Support</td>
<td>Government</td>
<td>Internet Vigilantism</td>
</tr>
<tr>
<td>Year</td>
<td>Group</td>
<td>Event Description</td>
<td>Type</td>
<td>Target</td>
<td>Motive</td>
</tr>
<tr>
<td>------</td>
<td>----------------</td>
<td>-----------------------------------------------------------------------------------</td>
<td>------------</td>
<td>--------------</td>
<td>--------------</td>
</tr>
<tr>
<td>2009</td>
<td>Australian government</td>
<td>Attacked Australian Minister's website in retaliation for Australian government's plans for ISP level censorship of the internet.</td>
<td>Harassment</td>
<td>Government</td>
<td>Coercion</td>
</tr>
<tr>
<td>2010</td>
<td>Operation Titstorm</td>
<td>Australian government sites being attacked for attempting to censor the internet.</td>
<td>Harassment</td>
<td>Government</td>
<td>Coercion</td>
</tr>
<tr>
<td>2010</td>
<td>Oregon Tea Party Raid</td>
<td>Attacked a social group to influence it to stop using Anonymous quote.</td>
<td>Harassment</td>
<td>Social group</td>
<td>Coercion</td>
</tr>
<tr>
<td>2010</td>
<td>Operation Payback</td>
<td>Retaliatory attack on Aplex software that launched DDOS attacks on websites that did not respond to software takedown notices.</td>
<td>Harassment</td>
<td>Corporate</td>
<td>Coercion</td>
</tr>
<tr>
<td>2010</td>
<td>Operation</td>
<td>Cyber attack on Quantico cyber communications.</td>
<td>Harassment</td>
<td>Government</td>
<td>Coercion</td>
</tr>
<tr>
<td>2011</td>
<td>Sony</td>
<td>As part of Operation Payback, Anonymous uses attacked the Sony PlayStation network and harassed Sony employees and members of their families.</td>
<td>Harassment</td>
<td>Corporate</td>
<td>Coercion</td>
</tr>
<tr>
<td>2011</td>
<td>Fine Gael</td>
<td>Attack on center right political party in Ireland.</td>
<td>Harassment</td>
<td>Political Group</td>
<td>Coercion</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Government</td>
<td>Coercion</td>
</tr>
</tbody>
</table>
Table 18. (continued)

<table>
<thead>
<tr>
<th>Year</th>
<th>Event</th>
<th>Description</th>
<th>Type</th>
<th>Target Type</th>
<th>Goal</th>
</tr>
</thead>
<tbody>
<tr>
<td>2011</td>
<td>Operation Tunisia</td>
<td>Targeted Tunisian, Egyptian, and Libyan Websites. Released names and passwords of government officials from Bahrain, Egypt, Jordan, and Morocco</td>
<td>Harassment</td>
<td>Government</td>
<td>Coercion</td>
</tr>
<tr>
<td>2011</td>
<td>HBGary Federal</td>
<td>Attack on executive who attempted to identify Anonymous uses</td>
<td>Harassment</td>
<td>Private Person</td>
<td>Coercion</td>
</tr>
<tr>
<td>2011</td>
<td>Westboro Baptist Church</td>
<td>Attack on Westboro Church website</td>
<td>Harassment</td>
<td>Religious Entity</td>
<td>Coercion</td>
</tr>
<tr>
<td>2011</td>
<td>Koch industries</td>
<td>Response to the Wisconsin protests by attacking a business owned by individuals who financially contributed to a lobby against unions</td>
<td>Harassment</td>
<td>Corporate</td>
<td>Coercion</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Harassment</td>
<td>Political Group</td>
<td>Coercion</td>
</tr>
<tr>
<td>2011</td>
<td>Operation Empire State Rebellion</td>
<td>Whistleblower action that exposed corruption and fraud in Bank of America</td>
<td>Social Justice</td>
<td>Corporate</td>
<td>Internet Vigilantism</td>
</tr>
<tr>
<td>2011</td>
<td>Sony</td>
<td>Announced intent to attack Sony websites in retaliation for Sony's gaining access to the IP addresses of all the people who visited George Holtz's blog. The group threatened to target Sony in response to what it perceived to be an act 'offensive against free speech and internet freedom.'</td>
<td>Retaliation</td>
<td>Corporate</td>
<td>Deterrence</td>
</tr>
<tr>
<td>2011</td>
<td>Spanish Police</td>
<td>DDoS attack on the Spanish Police website in retaliation for the arrests of three hackers</td>
<td>Retaliation</td>
<td>Government</td>
<td>Coercion</td>
</tr>
<tr>
<td>2011</td>
<td>Operation India</td>
<td>Cyber movement against corruption in India</td>
<td>Support</td>
<td>Government</td>
<td>Coercion</td>
</tr>
<tr>
<td>2011</td>
<td>Operation Malaysia</td>
<td>Attack on 91 websites on the Malaysian government for blocking websites such as WikiLeaks and The Pirate Bay</td>
<td>Harassment</td>
<td>Government</td>
<td>Coercion</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Retaliation</td>
<td>Government</td>
<td>Coercion</td>
</tr>
<tr>
<td>Year</td>
<td>Operation</td>
<td>Description</td>
<td>Target</td>
<td>Coercion</td>
<td></td>
</tr>
<tr>
<td>------</td>
<td>---------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>--------</td>
<td>-----------</td>
<td></td>
</tr>
<tr>
<td>2011</td>
<td>Operation Orlando</td>
<td>Operations against several Orlando websites to in retaliation against the arrest of members of ‘Food Not Bombs’ for feeding homeless in Lake Eola Park.</td>
<td>Retaliation</td>
<td>Government, Coercion</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Harassment</td>
<td>Corporate, Coercion</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Harassment</td>
<td>Religious Entity, Coercion</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Harassment</td>
<td>Social group, Coercion</td>
<td></td>
</tr>
<tr>
<td>2011</td>
<td>Operation AntiSec</td>
<td>Collaboration with Lulzsec to target corporate and government websites in the United States, Tunisia, Anguilla, Brazil, Zimbabwe, Turkey, and Australia.</td>
<td>Harassment</td>
<td>Government, Coercion</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Harassment</td>
<td>Corporate, Coercion</td>
<td></td>
</tr>
<tr>
<td>2011</td>
<td>Operation Facebook</td>
<td>Threat to attack Facebook.</td>
<td>Harassment</td>
<td>Corporate, Victimizing</td>
<td></td>
</tr>
<tr>
<td>2011</td>
<td>Operation Bart</td>
<td>Organization of Mass protests, email bombs, and release of BART personnel personal information in retaliation for shutdown of cell phone service to hamper protest activities.</td>
<td>Retaliation</td>
<td>Government, Coercion</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Retaliation</td>
<td>Private Person, Coercion</td>
<td></td>
</tr>
<tr>
<td>2011</td>
<td>Shooting Sheriff's Saturday</td>
<td>Hacking 70 law enforcement websites in predominately rural communities.</td>
<td>Harassment</td>
<td>Government, Victimizing</td>
<td></td>
</tr>
<tr>
<td>2011</td>
<td>Support of Occupy Wall Street</td>
<td>Support to the Occupy Wall Street movement.</td>
<td>Support</td>
<td>Corporate, Internet Vigilantism</td>
<td></td>
</tr>
<tr>
<td>2011</td>
<td>Operation Darknet</td>
<td>DDoS’d child porn sites and published the usernames of 1500 individuals and informed the Federal Bureau of Investigation and Interpol.</td>
<td>Social Justice</td>
<td>Social group, Internet Vigilantism</td>
<td></td>
</tr>
<tr>
<td>Year</td>
<td>Incident</td>
<td>Description</td>
<td>Motivations</td>
<td></td>
<td></td>
</tr>
<tr>
<td>------</td>
<td>----------</td>
<td>-------------------------------------------------------------------------------------------------------</td>
<td>------------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2011</td>
<td>Operation to Loz Zetas</td>
<td>Anonymous threatened to publish members of its cartel if it did not release a Anon member they had kidnapped</td>
<td>Retaliation, Social group, Deterrence</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2011</td>
<td>Operation Brotherhood Takedown</td>
<td>Attack on Muslim Brotherhood Websites Response to UC Davis pepper-spray incident</td>
<td>Harassment, Government, Coercion</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2011</td>
<td>John Pike Incident</td>
<td>Retaliation Government Coercion</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2011</td>
<td>Operation Deepthroat</td>
<td>Attack on 9gag Harassment Social group</td>
<td>Coercion</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2012</td>
<td>CLSEA hack</td>
<td>Attack on California Statewide Law Enforcement Association to protest police brutality Harassment Social group</td>
<td>Victimization, Government, Coercion</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2012</td>
<td>Occupy Nigeria</td>
<td>Attack on web assets of the Nigerian government in protest of the removal of fuel subsidies Harassment Government</td>
<td>Coercion</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2012</td>
<td>Operation Megaupload</td>
<td>Attacks on UMG, Dept. of Justice, U.S. Copyright Office, FBI, MPAA, Warner Brothers, RIAA, and HADOPI in retaliation for shutting down the share file site Megaupload Retaliation Corporate</td>
<td>Coercion</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2012</td>
<td>Anti-ACTA activism in Europe</td>
<td>Attack on Polish government websites</td>
<td>Harassment, Government, Coercion</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2012</td>
<td>Operation Russia</td>
<td>Attacks on pro-Kremlin activist</td>
<td>Harassment, Government, Coercion</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2012</td>
<td>Boston Police Department Attacks</td>
<td>Attack on Boston Police Department to protest eviction of Occupy Wall Street protestors Retaliation Government</td>
<td>Coercion</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2012</td>
<td>Syrian Government E-mail Hack</td>
<td>Hacking and posting on WikiLeaks 2.4 million emails form Assad's staffers</td>
<td>Harassment, Government, Coercion</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2012</td>
<td>AntiSec Leak and CIA Attack</td>
<td>Attack on CIA website</td>
<td>Harassment, Government, Coercion</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Year</td>
<td>Attack</td>
<td>Description</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>------</td>
<td>--------</td>
<td>-------------</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2012</td>
<td>Interpol Attack</td>
<td>Attack on Interpol in retaliation for arresting 25 suspected Anons</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2012</td>
<td>AIPAC Attack</td>
<td>Attack on American Israel Public Affairs Committee website</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2012</td>
<td>Vatican website DDoS Attack</td>
<td>Attack on Vatican website and radio station</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2012</td>
<td>Bureau of Justice leak</td>
<td>Stealing 1.7GB of data from U.S. Bureau of Justice</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2012</td>
<td>Taking down of Monsanto's Hungarian website</td>
<td>Collapsed Monsanto's Hungarian website</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2012</td>
<td>Symantec source code leak</td>
<td>Leak of source code for old version of Norton Antivirus and Norton Utilities</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2012</td>
<td>April 2012 Chinese Attack</td>
<td>Attacking 485 Chinese government websites to protest the lack of democracy.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2012</td>
<td>Operation Bahrain and Formula One Attacks</td>
<td>Protest of Bahrain Formula One which was sponsored by the government</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2012</td>
<td>Occupy Philippines</td>
<td>Attack on China Media Union website</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2012</td>
<td>Operation India</td>
<td>Attack on Indian Supreme courts and current-ruling Congress in retaliation for ISPs blocking video sites like Vimeo and file-sharing sites like the Pirate Bay</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2012</td>
<td>Operation Quebec</td>
<td>Attack on Canadian websites, and threats to Formula 1 Grand prix of Quebec in retaliation to legislation that would restrict freedom of association</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2012</td>
<td>Operation Japan</td>
<td>Attack on Japanese Business Federation</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 18. (continued)

<table>
<thead>
<tr>
<th>Year</th>
<th>Event</th>
<th>Description</th>
<th>Motivation</th>
<th>Type</th>
<th>Tactics</th>
</tr>
</thead>
<tbody>
<tr>
<td>2012</td>
<td>Operation Anaheim</td>
<td>Online protest in response to Anaheim police shooting. Also posted personal information of police chief John Welter</td>
<td>Social Justice</td>
<td>Harassment</td>
<td>Private Person</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Government</td>
<td>Social Justice</td>
<td>Coercion</td>
</tr>
<tr>
<td>2012</td>
<td>AAPT attack</td>
<td>Release of 40 GB from Australian ISP AAT to protest data retention policy</td>
<td>Harassment</td>
<td>Corporate</td>
<td>Coercion</td>
</tr>
<tr>
<td>2012</td>
<td>Operation Myanmar</td>
<td>Attack on Myanmar websites in protest for killing Muslim Rohingya Myanmar</td>
<td>Harassment</td>
<td>Corporate</td>
<td>Coercion</td>
</tr>
<tr>
<td>2012</td>
<td>Uganda LGBT rights</td>
<td>Hacking of Uganda government websites to protest country's anti-gay laws</td>
<td>Social Justice</td>
<td>Government</td>
<td>Coercion</td>
</tr>
<tr>
<td>2012</td>
<td>Hong Kong National Education</td>
<td>Protest of Government of Hong Kong educational curriculum</td>
<td>Harassment</td>
<td>Government</td>
<td>Coercion</td>
</tr>
<tr>
<td>2012</td>
<td>Release of Westboro Baptist Church Personal Information</td>
<td>Re-posting personal members of the Westboro Baptist Church</td>
<td>Social Justice</td>
<td>Religious Entity</td>
<td>Coercion</td>
</tr>
<tr>
<td>2013</td>
<td>Steubenville rape case</td>
<td>Released incriminating video and emails of attempted cover-up</td>
<td>Social Justice</td>
<td>Government</td>
<td>Internet Vigilantism</td>
</tr>
<tr>
<td>2013</td>
<td>Aaron Swartz Suicide</td>
<td>Attack on United States Sentencing Commission</td>
<td>Retaliation</td>
<td>Government</td>
<td>Deterrence</td>
</tr>
<tr>
<td>2013</td>
<td>Federal Reserve</td>
<td>Attack on Federal Reserve</td>
<td>Harassment</td>
<td>Government</td>
<td>Victimizing</td>
</tr>
<tr>
<td>2013</td>
<td>Operation North Korea</td>
<td>Declared cyber war on North Korea</td>
<td>Harassment</td>
<td>Government</td>
<td>Coercion</td>
</tr>
<tr>
<td>2013</td>
<td>Op Israel</td>
<td>Attack on Israeli websites</td>
<td>Harassment</td>
<td>Government</td>
<td>Victimizing</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Harassment</td>
<td>Corporate</td>
<td>Victimizing</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Harassment</td>
<td>Religious Entity</td>
<td>Victimizing</td>
</tr>
<tr>
<td>2013</td>
<td>2012 Cleveland police shooting incident</td>
<td>Release of personal information of two officers involved in police shooting</td>
<td>Social Justice</td>
<td>Government</td>
<td>Coercion</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Harassment</td>
<td>Private Person</td>
<td>Victimizing</td>
</tr>
<tr>
<td>Year</td>
<td>Event</td>
<td>Description</td>
<td>Type</td>
<td>Perpetrator/Actor</td>
<td></td>
</tr>
<tr>
<td>------</td>
<td>-----------------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>-----------------------------</td>
<td>-------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>2013</td>
<td>Retaeh Parsons</td>
<td>Threat to release personal information of perpetrators</td>
<td>Social Justice</td>
<td>Government Coercion</td>
<td></td>
</tr>
<tr>
<td>2013</td>
<td>Philippine Coast Guard Incident</td>
<td>Attack on Philippine government websites</td>
<td>Harassment</td>
<td>Government Coercion</td>
<td></td>
</tr>
<tr>
<td>2013</td>
<td>EDL</td>
<td>Publishing personal information of various English Defense League members online</td>
<td>Harassment</td>
<td>Political Group Coercion</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Social Justice</td>
<td>Political Group Internet Vigilantism</td>
<td></td>
</tr>
<tr>
<td>2013</td>
<td>Hawthorne dog shooting incident</td>
<td>Threat to post personal information of an arresting police officer</td>
<td>Social Justice</td>
<td>Government Internet Vigilantism</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Harassment</td>
<td>Private Person Victimizing</td>
<td></td>
</tr>
<tr>
<td>2013</td>
<td>Nigerian anti-gay laws</td>
<td>Attack on national website of Nigeria</td>
<td>Harassment</td>
<td>Government Coercion</td>
<td></td>
</tr>
<tr>
<td>2013</td>
<td>The GCSB</td>
<td>Attack on New Zealand Government Communications Security Bureau</td>
<td>Harassment</td>
<td>Government Coercion</td>
<td></td>
</tr>
<tr>
<td>2013</td>
<td>Operation Singapore</td>
<td>Attack on Singapore government, community sites, and newspapers</td>
<td>Harassment</td>
<td>Government Victimizing</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Harassment</td>
<td>Social group Victimizing</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Harassment</td>
<td>Corporate Victimizing</td>
<td></td>
</tr>
<tr>
<td>2013</td>
<td>Support of anti-PDAF movement</td>
<td>Hacking of Philippine government websites</td>
<td>Harassment</td>
<td>Government Victimizing</td>
<td></td>
</tr>
<tr>
<td>2013</td>
<td>Operation NSA</td>
<td>Announced intention to hack the National Security Agency</td>
<td>Harassment</td>
<td>Government Coercion</td>
<td></td>
</tr>
<tr>
<td>2013</td>
<td>Operation USA</td>
<td>Announced intention to attack government websites in retaliation for US military involvement in Afghanistan and Pakistan as well as expanded federal powers within the United States</td>
<td>Retaliation</td>
<td>Government Coercion</td>
<td></td>
</tr>
</tbody>
</table>

Appendix B: Social Scans

Figure 17. Twitter Feeds–Social, Posts Informing Community Members of Potential Government Action When Russia Attempted to Track TOR Users. This figure illustrates the sharing of police and law enforcement operations information (SDI2). Adapted from Anonymous (2014, July 29) Anonymous. Retrieved from Twitter: www.twitter.com.
Figure 19. Twitter Posts Containing Critical Commentary and Protests of the Killing of Palestinians by Israelis in Gaza. This figure illustrates the discussion of planned protest gatherings (SDI3). Adapted from Anonymous (2014a, July 30). Retrieved from Twitter: http://www.twitter.com.
Figure 20. Twitter Posts Containing Critical Commentary and Protests of the Killing of Palestinians by Israelis in Gaza. This figure illustrates the discussion of planned protest gatherings (SDI3). Adapted from Anonymous (2014b, July 30) Anonymous. Retrieved from Twitter: www.twitter.com.
Figure 24. Facebook Posts Containing Critical Commentary on Israeli Actions in Gaza. The comments are protesting the killing of civilians. This figure illustrates the discussion of planned protest gatherings (SDI3). Adapted from Anonymous (2014, July 30) Anonymous. Retrieved from Facebook: www.facebook.com.
Figure 26. Facebook Post From July 30, 2014, Containing Critical Commentary on Israeli Actions in Gaza. The posts are in protesting of the killing of civilians. This figure illustrates the discussion of planned protest gatherings (SDI3). Adapted from Anonymous (2014, July 30) Anonymous. Retrieved from Facebook: www.facebook.com.
Figure 27. Facebook Posts From July 30, 2014, Containing Critical Commentary on Israeli Actions in Gaza. The posts are in protest of the killing of civilians. This figure illustrates the discussion of planned protest gatherings (SDI3). Adapted from Anonymous (2014, July 30) Anonymous. Retrieved from Facebook: www.facebook.com.
Figure 28. Facebook Posts From July 30, 2014, Containing Critical Commentary on Israeli Actions in Gaza. The comments contain messages protesting the killing of civilians. This figure illustrates the discussion of planned protest gatherings (SDI3). Adapted from Anonymous (2014, July 30) Anonymous. Retrieved from Facebook: www.facebook.com.
Figure 29. Cyber Intelligence Sharing and Protection Act (CISPA) Commentary From July 30, 2014. This figure illustrates the promotion of protection of hacker community values (SDI1). Adapted from #OpCISA. Retrieved from RT:rt.com/usa/169888-anonymous-cybersecurity-bill-wrath.
Figure 30. CISPA Commentary From July 30, 2014. This figure illustrates the promotion of protection of hacker community values (SDI1). Adapted from #OpCISA. Retrieved from RT:rt.com/usa/169888-anonymous-cybersecurity-bil-wrath.
Figure 31. Protest of Israeli Actions in Gaza Posted on Twitter Addresses the Killing of Anon Members. This figure illustrates the discussion of planned protest gatherings (SDI3). Adapted from Anonymous (2014b, July 30) Anonymous. Retrieved from Twitter: www.twitter.com.
Figure 32. Commentary on Israeli/Palestinian Conflict Posted on 4Chan b Board. Comment contains critical commentary on Israel and Palestine. This figure illustrates the encouragement of political activism (PDI1). Adapted from Random Board. Retrieved from 4chan: boards.4chang.org.
Figure 33. Commentary on Israeli/Palestinian Conflict Posted on 4Chan b Board. Posts contain critical commentary on Israel and Palestine. This figure illustrates the encouragement of political activism (PDII). Adapted from Random Board. Retrieved from 4chan: boards.4chang.org.
Figure 34. Promotion of the Hacker Values of Freedom of Information and Transparency of Government. This figure illustrates the promotion of protection of hacker community values (SDII). Adapted from Anonymous (2014, August 1) Anonymous. Retrieved from Twitter: www.twitter.com.
Figure 35. August 7, 2014. Facebook Commentary Calling for Attacks on the NSA, IRS, EPA, and Other Government Agencies. This figure illustrates the discussion of future targets (SDI3).

Adapted from Anonymous Operations. Retrieved from Facebook: