5-2010

Bits and Bytes on the Front Lines An Examination of Distributed Denial of Service Attacks as a Terrorist and/or State-Based Threat

Ben Spear

University at Albany, State University of New York

Bits and Bytes on the Front Lines

An Examination of Distributed Denial of Service Attacks as a Terrorist and/or State-Based Threat

Ben Spear

Honors Thesis

March 10, 2010

Introduction

Recently in the news there has been a focus on the threat of cyber tactics. People hear terms like “cyberterrorism,” “cyberwar,” and “digital Pearl Harbor.” These terms all fall under the same subject of Information Warfare or Information Operations as the military terms it. Just this past year blogs, news sites and papers were filled with fantastical stories of the vicious cyberwar that paralleled live military action between Russia and the former Soviet republic of Georgia. The 2007 attack on the Internet infrastructure of Estonia is perhaps the most prevalent attack to date, mostly because it resulted in the entire Internet of that country being shut down. But how real is the threat of cyberterrorism and information warfare?

For years the term “hacking” has been misused to describe actions by an individual or groups of individuals that partake in the malicious use of tools to disrupt the Internet. Hacking has been in existence since the beginning of the computing age. The term originally, and those among them would argue to this day, refers to people who tinkered with computers or software in order to open them up to their full potential. A number of these tinkerers sometimes used their skills just to show those in the community how knowledgeable they were. Perhaps one of the earliest known hacks was one that made long distance calls on AT&T free, part of the phenomenon known as “phreaking”.

As computers became more readily available, those who participated in phone phreaking applied their skills to the new medium. With the rapid spread of the Internet in the 1990s via the World Wide Web a whole new world was opened up. The more complex the technology the more open and greater the vulnerabilities and this was most definitely the case after the release of the World Wide Web in 1993. Those early phreakers and the successive generations took advantage of these vulnerabilities, once again trying to prove their skills to their colleagues and earn a reputation. Soon though the hacker world developed into two camps, white hats and black hats. White hats are those hackers that are often employed by a security firm or the government, and sometimes are just regular individuals who attempt to find vulnerabilities and report them. Black hats are those hackers that try to exploit vulnerabilities, often maliciously for personal gain, earning them the separate distinction of being called crackers.

As I’ve already iterated, most hackers are looking to exploit vulnerabilities so that they can report them, or to prove something to their friends but recent events have seen the skills of hackers used for more malicious purposes. The past decade has seen the growth of the Internet as a medium for communication and activist groups have taken hold of this use wholeheartedly. The presidential campaigns of Howard Dean and Barack Obama are testament to this fact. But while some activist groups use the Internet for traditional activist means such as fundraising and awareness, others use the hacker arsenal in order to have their grievances addressed. The case of the Zapatista movement in Mexico and the hijacking of the WTO site in 1999 are just some examples of this evolution in activism, or what Dorothy Denning has called “hacktivism” (D. E. Denning 1999). The 2007 attack in Estonia, which has proven to be the work of angered ethnic Russians living there, also highlights how the Internet can be used maliciously. More recently there was a hack attack launched against the Internet search and services giant Google, within China. The attacks have been purportedly sourced to two schools in China that specialize in computer science and training military specialists (Rubin 2010). Google has gone so far as to threaten abandonment of the market if the situation in China does not change. For the time being they have removed their censorship of their Chinese services. All of these instances show how significant this threat may be.

It is events like these that cause people to become concerned about the cyber threat and in a post-9/11 world the fear of this threat has grown to include the use of these tools by terrorists. Some people are concerned that terrorists will use the Internet to attack our infrastructure, cut power, and cause planes to crash. At the same time the media continues to prey on this fear posting stories about large cyber-attacks and hyping up their effects. While terrorists may use cyber tactics in the future, the other definite threat comes from other states and their military and intelligence services. The United States has developed a Cyber Command from which to defend military systems and prepare their own attack plans. Other countries such as Russia and China have also invested money in this new form of Information Warfare. As we move into a new era of warfare much is unknown, we must understand this form of warfare and how our adversaries intend to use it in order to determine how we should use it ourselves.

Statement of the Research Question

For the past few years now I have studied the phenomenon of cyber-attack. As the engagements in Estonia and Georgia unfolded, as well as recent events concerning China, three key questions arose related to cyber-attack. The first question was who is committing these attacks? Are they states, terrorists, civilians? This is an important question to answer but it seems that it would be difficult to fully answer. If we are to understand attacks, how they work and how they are formulated we must also understand who is committing them. An attack by a terrorist might be carried out much differently than one by a hacker. In an extension of this my second question was why do people carry out cyber-attacks? What is their motive? Motive is important in understanding attacks because it may determine a number of variables concerning the attack such as target, length and strength of attack. What motivates someone to commit an attack also motivates how they attack. Lastly, how serious are these attacks? Is anyone getting hurt? Is there a lot of monetary damage? It’s important to look at how damaging these attacks are now to help extrapolate how big of a threat they are and will be.

My first attempt at answering these questions came in a case study of the Estonian Cyber War in which I used process tracing to speculate on the probable perpetrators of the attack. Through the use of news articles and network security reports I was able to determine that the Russian government was not the source of attacks but rather it was ethnic Russians collaborating on Internet forums and sharing information on how to launch an attack (Nazario, DDoS Attack Evolution 2008). These non-state actors were politically motivated by the moving of a Soviet-era World War II memorial to take action against their government (Landler and Markoff 2007).

While the process tracing provided me with valuable insights these questions are also usefully investigated looking across a variety of cyberterrorist cases. What I have chosen to do is expand my work on Estonia to include all attacks of that nature, specifically distributed denial of service or DDoS attacks. This particular form of attack has become very popular in the past decade, starting with the MafiaBoy attacks in 2000, and more recently the Russian-Georgian Conflict (Richtel 2000, Tabatadze 2008). The attack involves an attacker collecting a number of slave computers into a botnet, usually through installing malware on those computers unauthorized, and using those slaves to issue requests to a target server. The high number of requests is eventually too much for the server to handle and so it shuts down preventing anyone from accessing it. (Paxson 2001) Sometimes these attacks can be so damaging that they will actually result in the need for new hardware. This is one of the many areas where monetary damage can enter the picture. While there are benign forms of DDoS caused by a popular website attracting more of an audience than it can support, more often than not it is a malicious attack meant to disrupt services and sometimes it can cause damage.

Literature Review

This research seeks to answer the question of who commits attacks and why through the lens of the DDoS attack, which is currently perhaps the most harmful of cyber-attacks. The literature on DDoS attacks themselves is limited to technical engineering papers in the computer science field on how these attacks are executed and how they can be combated. In order to gain an understanding of the academic field surrounding this topic we must look to general research on cyberterrorism and information warfare as a whole. But before we begin to look at what other scholars say about cyberterrorism and information warfare we must understand what these terms mean. The term cyberterrorism, as the literature suggests, is very broad and loosely defined. In my review it was not uncommon to find 5-10 different definitions and all of the literature belabored this point. For this research I have chosen to use a commonly cited definition given by Mark Pollitt of the FBI. This definition combines the definition of cyberspace given by Barry Collin and the U.S. Department of State definition of terrorism: "Cyberterrorism is the premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against noncombatant targets by sub national groups or clandestine agents" (Pollitt 1998). This very narrow definition allows for a focused research topic.

Defining information warfare is much easier as the Joint Command of the U.S. military has defined it in an operations manual as "the integrated employment of the core capabilities of electronic warfare, computer network operations, psychological operations, military deception, and operations security, in concert with specified supporting and related capabilities, to influence, disrupt, corrupt or usurp adversarial human and automated decision making while protecting our own" (Joint Publication 3-13.3: Operations Security) According to the military this includes signals intelligence, electromagnetic pulses and other older forms of warfare. Within this definition the kind of attacks being researched here is computer network operations (CNO), specifically the sub-capability of computer network attack. There is also computer network defense which is an important capability as threats begin to materialize further. Terrorist organizations are known to use other forms of information warfare outside of CNO and this will be discussed further (D. E. Denning 2005).

In a review of the literature there were a number of common themes. A majority of the literature came from a small number of scholars. Literature written by other scholars saw this core group cited often. What was often discussed is what is so enticing about cyber-attacks that individuals use them. The literature overwhelmingly agrees on the main benefit of cyber-attack, which is its low overall cost, both in terms of cash and in general terms. In terms of monetary cost, it is quite cheap to purchase a computer today with systems as low as $200 being sold. A simple computer is all one needs to launch an attack and there is no cost for software because the tools for cyber-attacks are freely available on the Internet (D. E. Denning 2009). Such programs are also quite easy to use. In addition to this there is also the possibility of using computers at an Internet café (Lawson 2001). These public spaces are often very cheap to rent time for usage and may also provide for anonymity.

Anonymity is one of the greatest benefits of cyber-attack, even if the attacker is not in an Internet café, and the literature discusses this at length (Wilson 2007). Most attackers will often route their attacks through different computers and IP addresses or proxies, in different cities, states and countries or use a system of botnets to hide the original actor. These practices make it very hard for victims or investigators to trace the source of a DDoS attack. In addition, the current statutes dealing with Internet crime or lack of them further hamper efforts. In the United

States for instance, one requires a warrant from every jurisdiction the IP trace passes through making it very difficult if at all possible to even begin a search for the culprit. This results in cases that are rarely solved. In the event of large attacks though it seems that national authorities become involved and may find the attacker, as was the case in the MafiaBoy incident in 2000.

Perhaps the biggest benefit of cyber-attack that greatly reduces cost is the ability to attack remotely. An attacker, in most cases, does not have to be on premises to launch an attack. This provides that travel does not need to be paid for and more importantly an attacker does not have to risk their life in an attack. This is an important advance in the case of a group like al-Qaeda, which relies on suicide bombers as they no longer need to expend lives for an attack. At the same time this is connected to the earlier discussion that cyber-attacks may not be as effective as terrorist groups want. It may be beneficial for a terrorist organization to not suffer from such an attrition of members but there is the tradeoff of effectiveness. Perhaps they are looking for some people to die, which has not occurred from a cyber-attack. Perhaps they might not get as large of a public response because cyber-attacks aren't necessarily reported or large enough to be of concern. The actual facts are that so far terrorist organizations have yet to attack via the Internet and it is quite possible that they never will because of a lack of effect (Lewis 2002, Conway 2007).

This leads us to ask what do terrorist organizations use the Internet for? The literature is very effective in answering this question. Currently terrorist organizations use the Internet, much like anyone else, as a means of communication. There are al-Qaeda websites, forums and chat rooms, as well as Internet newsletters (Weimann 2006). Furnell and Warren tell us that terrorists can use the Internet to "raise funds for their cause" and that it is "the ideal propaganda tool for a terrorist" (Furnell and Warren 1999). It is also well known that the 9/11 hijackers coordinated the attack and other information regarding it through emails and other forms of Internet communication. The use of newsletters as described before can be used as propaganda in al-Qaeda areas to better attract the populace. Al-Qaeda is also known to employ individuals that are able to forge electronic documents and encrypt communications. These agents also have skills in breaking encryption, which could be used for intelligence work (Weimann 2006). At the same time, while they might not use the Internet aggressively at the present that does not mean this will always be the case. Terrorist groups have shown an interest in the Internet as a weapon and as a target, possibly using these tools against critical infrastructure (Weimann 2006). Some have also argued that terrorists just do not have the skills to launch a viable cyber-attack and might hire hackers to develop attacks for them but Conway counters this by arguing that it is much harder to get a hacker to cross the threshold from launching attacks on computers to launching attacks that could be damaging (Conway 2004).

This information begs the question, if not terrorists, who is using cyber-attack and why? Most of the literature suggests that cyber-attacks are politically motivated. In fact most attacks are of a "hacktivist" nature (D. E. Denning 1999). Hacktivists as the name suggests are hacking activists who use the tools of the Internet to gain attention to their cause. Common hacktivist tactics include web defacement and email bombs, and sometimes they have used DDoS (Nagpal 2002). Examples of hacktivist action include the web sit-ins of the Zapatista movement and WTO trade talks as well as DDoS attacks related to the bombings in Kosovo (Nagpal 2002). It is quite understandable why someone with a goal might seek to use these tools as a form of protest. In live protests some participants often become rowdy and in much the same sense some members of a group with an online petition and movement might become aggressive on the Internet.

Another motive for cyber-attack seems to be criminal. The possibility was discussed regarding the Estonian attacks and it is very popular in general. Syndicates like the Russian Business Network have been cited as sources of attack before and it is not surprising that this will continue (Shachtman, Top Georgian Official: Moscow Cyber Attacked US-We Just Can't Prove It 2009). As early as 2000, officials were concerned about the use of the Internet for the purposes of extortion and the possibility of this threat continues to exist today (Freeh 2000, Wilson 2008). The botnets controlled by crime syndicates such as the Zhelatin gang's Storm botnet are strong enough to keep a site down for days. The threat of cyber-extortion is enormous as the use of cyber-attacks to enforce requests may cause a site to go down indefinitely. Syndicates use the strength of their botnets to extort money from gambling websites (Haug 2007). Such sites rely on the strength and trust of their customer base to continue business, which requires them to maintain continuous operation. Should a gambling site be shut down for even a short period of time it could/would be quite damaging to their customer base as users leave in droves for fear of their money disappearing or not having access to the services. Mirkovic and Reiher discuss this possible loss of trust as a reason for the lack of reporting concerning attacks, as companies fear the end result (Mirkovic and Reiher 2004).

The possible economic loss from a cyber-attack is sometimes unfathomable, the five most costly viruses of all time summed to $102 billion in losses (Borglund 2009). The most expensive single virus was MyDoom at $38.7 billion (Borglund 2009). While the economic motive for a cyber-attack might also be common, most attacks of an economic motive would most likely be in conjunction with an attack that had a political or criminal motive, the true motive being to see the victim suffer financially or to enhance the attacker financially. Economic motive does not seem to truly be that much of a threat singularly.

Based on this literature I was able to form two hypotheses regarding DDoS attack. The first is that if there is a DDoS attack, then it will be politically motivated and hacktivist in nature. Such groups have used the Internet more popularly and are also known to have launched attacks. While economic and criminal attacks are sometimes better reported it is political attacks that seem to have the largest following and I hoped to test that notion with this research. In what is really a continuation and reinforcement of my first hypothesis, I also hypothesized that if there is a DDoS attack, then it will be committed by a non-state actor. Attacks such as in Estonia and by the Zapatistas, and a lack of real cyberwars led me to argue such. Even if I found a number of terrorist attacks, which is what I hoped, these would also fall under the non-state moniker. My own hopes for the research and the literature strongly supported the formulation of this hypothesis.

After examining what makes cyber-attacks alluring and who uses them, perhaps the most popular theme was relating to the threat of cyber-attack. Most common in the media, and no differently in the literature, are discussions of potentialities such as hackers being able to access the control systems for a transit system or power station and being able to manipulate them to create havoc (Collin 2004). In contrast though, most of the literature argues that such a threat does not actually exist and some would offer the fact that no threat has yet materialized as proof of this (Jones 2005). Maura Conway in *Cyberterrorism: Hype and Reality* tells us that sensationalism in the media and sometimes in academia is so overblown, that in reality the magnitude of the threat is hard to pin down (Conway 2007).

Gabriel Weimann in his book *Terror on the Internet* challenges the media on this because they “fail to distinguish between hacking and cyberterrorism and exaggerate the threat of the latter” (Weimann 2006) He also discredits the arguments of some scholars about the vulnerability of SCADA systems which control utilities and other forms of critical infrastructure such as the air traffic control (ATC) system. Other scholars argue that planes could be made to crash if the ATC system were hacked and taken control of. (Weimann 2004) These threats are greatly exaggerated as systems such as power and ATC are run on antiquated hardware before the age of the Internet. As such they are not connected directly to the Internet, but rather "air-gapped," much like the nuclear arsenals of the United States which some people have been concerned about. (Weimann 2006) He also says that such systems require a large amount of human interaction and as so any discrepancies from an intrusion would be noticed fairly early (Weimann, Cyberterrorism: How Real is the Threat? 2004). Another scholar points out "while many computer networks remain very vulnerable to attack, few critical infrastructures are equally vulnerable" (Lewis 2002).

In addition to this threat assessment the literature also discounts the threat of cyber-attacks as unable to create the kind of damage that a physical attack might incur. No one, as much of the literature mentions, has yet to die of a cyber-attack. Another notion, as put forth by Dorothy Denning, is that "it is not clear that a repeat attack in cyberspace would have as much impact" (D. E. Denning 2009). The argument behind this is that once a country is attacked once it will increase its defenses to prevent another attack. Other countries may also increase their defenses as a result. This is supported by the events in Estonia and Georgia where due to the attack on the former the latter was more prepared to defend and counter-attack. In addition, Estonia itself has greatly increased its defenses and become more connected to the networks of other countries so that it could better fend off an attack. In fact, the Estonian attacks continue to this day and this increased cooperation and preparation allows for the attacks to go unnoticed. (Nazario, DDoS Fines in Estonia 2008)

These discussions of how severe an attack might actually be led to the formulation of my third and final hypothesis, if there is a DDoS attack, then it will be of negligible severity. The literature very plainly shows this to be true and I expected my results would show the same. Much of the literature discounted the threat of attacks as usually being nuisances or disruptions and not much of anything (Cortes 2004). A number of scholars even used this as an argument that cyberterrorism does not exist because it cannot be used to threaten violence. James Lewis tells us that cyber-attacks are ineffective because they usually are singular events whereas a physical attack is only effective after repeated efforts (Lewis 2002). He pointed to studies on the mentality of Germans in response to air attacks during World War II to support this fact. He elaborates on the theme of cyber-attacks as mere nuisances arguing that even if critical infrastructure were taken down it wouldn’t impact the minds of Americans. He argues that events such as occasional blackouts are seen as routine to most Americans and would not merit much of a response, which is what terrorists are looking for (Lewis 2002).

This brings us to another theme of the literature that cyber-attacks do “not have the same dramatic and political effect that terrorists seek” as compared to physical attacks (Lewis 2002). As such a number of scholars believe that terrorists would not be interested in cyber-attacks as a primary form of attack, though it has been suggested that they might use it to support a physical attack to create more chaos. At the same time the disruption of attacks does have the potential to cause disruptions elsewhere. As the Estonian attacks suggest, an attack could certainly cause financial damage. The populace relies on a number of websites for services and should those services be interrupted it could result in the loss of large amounts of revenue for a company. At the same time because these people rely on these services they must have a great deal of trust to be handing out their private information. An attack of a certain magnitude may result in a loss of trust in the system that would lead to negative long-term effects for not only the Internet economy but also the economy as a whole (Karatzogianni 2002).

It's fair to say that there is a lot of discussion of the threat of cyberterrorism and information warfare in the literature but at the same time, just because the threat isn't large now does not mean it cannot be in the future. A report on cybersecurity prepared for President Obama notes that "foreign entities have been able to penetrate poorly protected computers and collect immense quantities of information" and that "exploiting vulnerabilities in cyber infrastructure will be part of any future conflict" (Lewis 2008). All points considered it seems that the threat of a cyberterrorist attack is not as high as some, such as the media, would argue. Hype is a very large issue in the field of cyber-attack. News organizations are very keen to jump on a story about minor hackers and refer to them as terrorists but as the literature argues minor hack attacks could never be considered a terrorist attack. News organizations reporting on such attacks create the image of a greater threat but at the same time the U.S. government is concerned and is working to combat any possible threat (Orlando 2009).

In the area of information warfare there has been no officially recognized attack by one foreign government against another to date but certain events are of questionable concern. For instance, some have blamed the Russian government for the Estonian and Georgian attacks, though there is no proof, and Burma has been accused of launching an attack on some sites (Burma Government blamed for attack on website of exile radio, TV 2009, Swaine 2008, Traynor 2007). It is well known that foreign governments are developing systems to engage in forms of information warfare. Besides the United States, Russia and China are also known to be developing cyber-capabilities and while not launching attacks they have been known to quietly enter systems and leave them unharmed, sometimes attempting to steal data (Gralla 2009, Report: Cyberspy network targets governments 2009, Gorman 2009, Cortes 2004). Since there has not officially been an attack the literature on information warfare is very similar to that of cyberterrorism and discussions on its uses are rather similar.

Methodology

In researching the use of cyber tactics by terrorist and government organizations I focused in on the subject of DDoS attack. This is the attack that would most likely be able to cause the damage on a scale that might call attention to the issue. As discussed earlier I sought to understand who uses cyber-attack, what motivates them to attack and how severe attacks are. The literature is very clear in its description of cyber-attacks to date. There has not been a truly damaging attack in the sense that no data has been lost or computers destroyed, but rather revenue is lost due to lost productivity. In addition to this terrorists have yet to launch an attack and if official word is to be believed, neither have states. Hacktivist attacks such as defacement seem to be most popular.

This research sought to test the three hypotheses by studying reported attacks. A review was done of news articles from 1995-2008 using LexisNexis. The starting date of 1995 was chosen because this is when the World Wide Web became commercially popular due to the release of Windows 95, which included the first release of Internet Explorer. This milestone made the Internet a viable target. Over the next five years there were a number of denial of service attacks by single individuals but around the dawn of the millennium this expanded into the distributed nature I studied. The period started with the large MafiaBoy attacks in 2000 and ended with the Georgian attacks in 2008. From the articles I extracted a number of important data points including the date/year of the attack, who attacked, who they attacked, why they attacked, how long they attacked and how severe was their attack. All these data points were important in answering my questions and proving/disproving my hypotheses. There were some problems in collecting the data. In the 15 year period I was only able to find news articles on thirty attacks and in addition to this I was unable to find all the data points for every attack. In this case one of DDoS' strengths, anonymity, hindered my ability to track down a large number of attacks. In terms of major attacks there could be anywhere from zero to thousands of attacks missing. As I reported earlier, many corporations will not report they were attacked because they are worried about their reputation. At the same time they might not have noticed they were attacked because they have so many servers that such an attack is absorbed. This was the case with an attack on the actual root servers that control traffic on the Internet. Users did not feel the pain of this attack because of the built in redundancy of the network. Due to the low number of recorded attacks I was unable to do a full statistical analysis but instead had to rely on just a basic descriptive understanding of the data.

Within the different data points I had various possibilities, for instance there could have been political, economic, criminal or traditional hacker motives. Possible targets included commerce, government, rival groups, religious organizations or the media. Severity was measured in terms of monetary damages as reported in the article or estimated based on length of attack and target. Actors included state actors and a division of non-state actors into terrorist, criminal or civilian actors, while length was measured on a scale of 1-10+days.

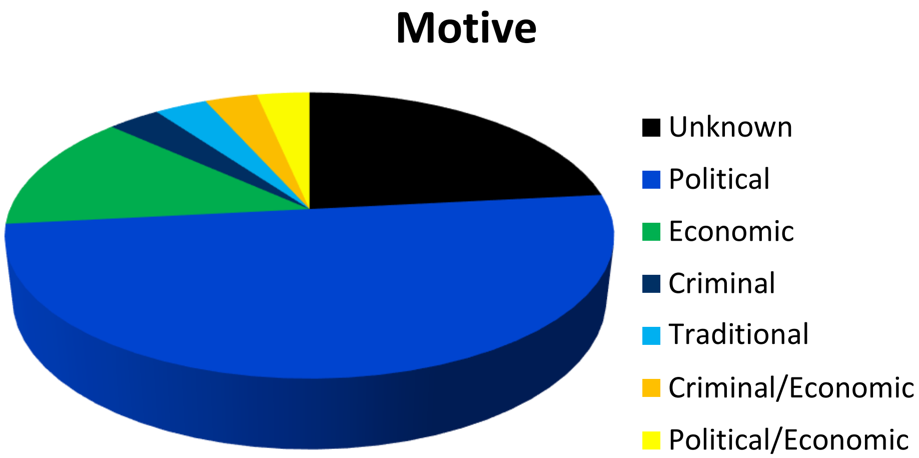
Giving a brief overview of the data, most of the articles came from newswires and attacks were launched against targets in the United States or in Europe. This makes sense as they are among the most Internet connected regions of the world. They are also regions where society is more open and so attackers, who the literature suggests are hacktivists, might be more inclined to launch an attack without fear of retribution from the target. The data was pretty evenly spread out across the timeframe of the past decade. All attacks happened within the 2000s and while spread out there was a bias towards the beginning and end of the time period. This is most likely because DDoS became quite prominent in the public at those times. The first attack, MafiaBoy, led to widespread news coverage for over a year, after which point attacks only tended to generate one article. At the other end of the timeline is the increasing cyberwarfare craze led by the Estonian and Georgian attacks as well as Barack Obama's cybersecurity initiative.

Results

After collecting the data and analyzing it, a number of themes were clear. As the literature suggested would be the case, most of my hypotheses were strongly supported by the data. The first hypothesis, if there is a DDoS attack, then it will be politically motivated and hacktivist in nature, was partially supported by 57% of the data. The question of a hacktivist attack was less conclusive due to the information available regarding actors. The second, if there is a DDoS attack, then it will be committed by a non-state actor, was strongly supported by the data with 87% of attacks, of the available data, being committed by non-state actors. The third hypothesis, if there is a DDoS attack, it will be of negligible severity, was also strongly supported with 57% of attacks being of a low severity.

The data regarding the first hypothesis, on motive, showed that 57% of attacks were of a political origin, 20% were of economic origin overlapping with criminal motive, and just one case was traditional hacking. The chart below illustrates these facts. The one hacker case was the first recorded DDoS attack known as MafiaBoy, which suggests there may be a trend regarding motive, in which there has been a shift over the past decade. Politically motivated attacks did not appear until a few years into the decade with a number of attacks in 2003, surrounding the Iraq War. The Cyber Intifada started in 2001 and continued throughout the decade (Lawson 2001).

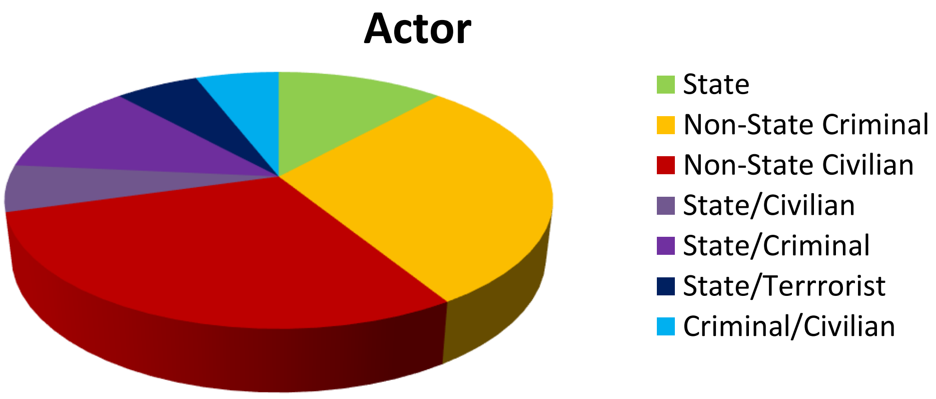
The large number of politically motivated attacks is interesting in that depending on the actors involved it may suggest a social movement mentality among actors.



The number of attacks with a solely economic motive was quite interesting in that I didn't expect there to be a high number of attacks as a number of economic attacks would have had a criminal motive. Attacks that fell under economic motive included one against the site of Virgin America on its launch day and one against the Million Dollar Homepage. These were attacks meant to financially harm the hosts of those sites. For instance, the attack on the Virgin website prevented anyone from booking flights on the airline on its first day of operation. The Million Dollar Homepage was a popular web meme created by an individual to sell ad space. These two attacks do not seem to have any criminal motive but are rather just trying to disrupt large public events, and were perhaps executed by traditional hackers.

At the same time, a majority of economically motivated attacks were of a criminal nature. These attacks were usually against gambling sites, in attempts to extort money from hosts for the benefit of crime syndicates. The syndicates which long have been known for their protection rackets in the physical world have transferred their business to the new digital medium. Instead of using bats to cause damage they use bits. Crime syndicates have also been known to use their botnets against each other, “going to the mattresses” in cyberspace. This was the case in a DDoS exchange between the Storm and Stration botnets, two systems controlled by competing Russian crime syndicates. The actions of criminals on the Internet are something that must be watched in the political arena as well though. Recent events suggest that criminal syndicates may have been involved in the Estonian and Georgian attacks either directly or indirectly. Indirect involvement refers to the possibility of criminal syndicates leasing time for the use of their botnets to other individuals to launch attacks. This is a grave threat as these botnets are very powerful and can be used to take down a large number of systems for extended periods of time.

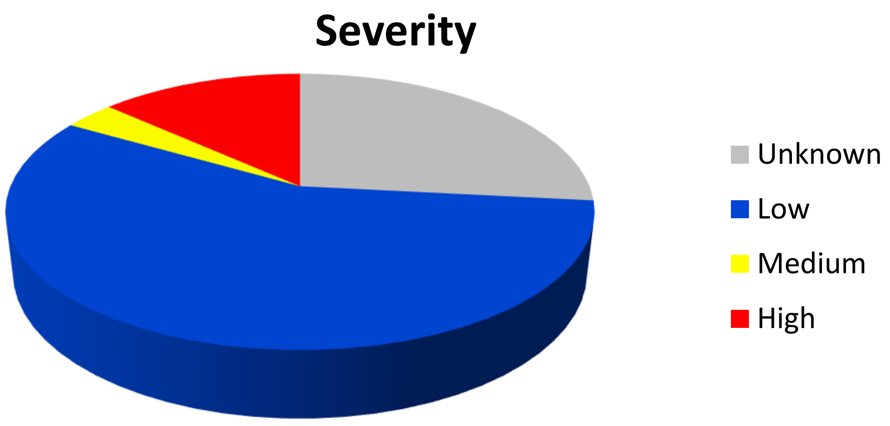
The data regarding actor was somewhat inconclusive as the anonymous nature of DDoS attacks resulted in 43% of the attacks reporting no attacker. Of the 64% of attacks where an attacker was reported 12% may have been state based and 29% of attacks were either criminal or civilian respectively. Another 29% of attacks appeared to be an overlap of criminal, civilian or state-based attacks. The chart below illustrates these facts. It is rather interesting to see such a large number of criminal attacks though not as surprising after reviewing the motive data. The criminal threat has been belabored enough though and we must focus on the civilian and possible state threat.



As the literature suggested a large amount of the attacks were committed by non-state actors but on the matter of whether the attacks were hacktivist the data was inconclusive. An equal amount of attacks were hacktivist as they were criminal. The hacktivist nature of DDoS attacks, similar to that of regular cyber-attacks is important as it shows the growing use of the Internet by individuals and interest groups in order to get their grievances addressed. A number of groups in the United States and elsewhere have looked to the Internet for mobilization, creating online petitions and hosting forums for discussion. The presidential campaigns of Howard Dean in 2004 and Barack Obama in 2008 are great examples of this expansion in the use of the Internet by individuals and groups. What this data shows is that these methods of social organization that have become popular can also be used for malicious purposes.

Perhaps the most interesting of all the data is the 12% of purportedly state-based attacks. Based on the literature such a large percentage was not expected. It seems from the data, that there is an evolutionary trend in the actors involved. The first attack was hacker related but this tactic was soon adopted by civilian actors. Criminal actors began using the tactic sometime later and only recently have state actors been implicated in an attack. This increasing trend towards state based attacks must be closely followed as it signals the move by countries like the United States, Russia and China towards greater use of asymmetric warfare. To date the number of attacks by states is very small but it will only increase to represent an equal third of the pie, and possibly more. In addition, attacks that are more definitively state attacks have been of a low severity so far, though there is no doubt that the severity of attacks will continue to climb.

The data regarding my last hypothesis, if there is a DDoS attack, it will be of negligible severity, like actor, was somewhat inconclusive due to the lack of information. Often information regarding damage was not recorded at the time of press because the extent of damage could not yet be determined or was irrelevant. For the purposes of this study severity was measured in terms of dollar denominated values as a result of damaged equipment or loss of productivity. An attack could have been of low, medium or high severity with low accounting for attacks causing $0-100,000 worth of damage, medium $100,001-1,000,000 worth of damage and high representing damages of $1,000,001+. 73% of the data was able to present us with information regarding severity with 78% of the available data showing attacks of a low severity, 3½% of the attacks being of a medium severity and 14% of attacks being of a high severity. The chart below illustrates these facts. It would seem that the literature was right in discrediting the hype of the media as such a high number of attacks had very little significance.



So far most of the hacktivist attacks and all the purportedly state-based attacks have been of a low severity. In regards to the hacktivist attacks this seems to make sense as those involved are most likely launching random attacks and not engaging in much preparation before doing so. The literature supported this fact as well as it supported low state involvement such as infiltrating systems while not damaging them. Interestingly the most severe attacks were those committed by criminal actors or traditional hackers. The trends suggest that the more resources or preparation for an attack the more severe the attack will be. This sets up an interesting possibility. While state-based attacks to date are of a low severity they have the potential to become the most severe of attacks. The most severe attacks seem to have required a large number of resources and preparation which are readily available to states. The amount of damage created by attacks like Estonia and viruses like MyDoom are only a brief foreshadowing of the damage that can be created by an attack launched by a state. States have even greater resources and time to prepare than criminal syndicates or hackers and so they have the potential to launch attacks that could keep a system inoperable for weeks and possibly even months, as opposed to days.

While having examined the data supporting my hypotheses there were some other interesting data points, in particular target and length of attack. As would be expected based on the typically political nature of cyber-attacks, most of the attacks were on commercial or government targets. There were also a number of attacks on the media. This is very significant as clearly those who are attacking wish it to garner greater publicity. Such attacks may create large enough a revenue loss or garner enough attention that the target may address the attacker's grievances. It is not surprising that the media hypes the threat of cyber-attack as large considering they are the target of a number of attacks. It is something that affects them every day. Media may also be attacked due to a difference in opinion regarding reporting. A number of the media DDoS attacks were against sites like that of Radio Free Europe (RFE) or a democratic advocacy site in Burma (Burma Government blamed for attack on website of exile radio, TV 2009, Mills 2008). These attacks support the increasingly political motive of attacks and in the case of the RFE attack a more hacktivist nature.

What is interesting is that attacks on government sites have only developed recently. There are a number of possibilities to discuss this phenomenon such as the exhaustion of other means of grievance but more than likely this has to do with the increasing presence of the government on the Internet. A number of states are seeking to become more connected and interactive with their citizenry. This openness makes government sites very prominent targets for attack.

Another popular target was the Internet infrastructure and Internet security firms. While popular these attacks ultimately fail because of the way in which the Internet was designed, to be redundant and resilient. The targets are firms that track those who commit attacks and sometimes even against the main root servers that direct all traffic on the Internet (Ingram 2007). There are thirteen of these servers located across the world, a majority in the United States. These servers are redundant and also backed up so that only a large, planned attack against them could possibly bring them down, and in turn reduce the capacity of the Internet. While the attacks that have occurred so far have failed that does not mean someone couldn't try to launch an even larger attack that might be successful. In fact it is certainly possible that if a war were to take place a state might seek to take down the entire Internet or at least the root server that serves the enemy state in order to disrupt operations.

Perhaps the most interesting of the other data points was the length of attack. Measured on a scale of 1 to 10+ days most of the attacks lasted only a day and an equal number of attacks lasted either 2-4 days or 10+ days. This suggests that most DDoS attacks sought only a minor effect. Of the attacks that lasted for only a day, most lasted for only hours. This shows that either the attackers did not have the resources to have an extended attack or they sought to just be a minor disturbance. I'm inclined to support the latter based on the large number of civilian actors reported in the data. Of those attacks that lasted for a number of days one was the MafiaBoy incident, another was a hacker worm called Code Red, and the last two were attacks on minor organizations. From this data I cannot posit any reasons as to why these attacks lasted longer than others.

The attacks that lasted for more than ten days were major attacks that occurred recently, and in some cases are still ongoing. These attacks included the Estonian attacks, the Georgian attacks and the Cyber Intifada, and their longevity suggests something very important to us. These attacks required mass organization and planning ahead of time and they used a large number of resources. To this day Estonian sites are still attacked every second, but they have built up a redundancy system to prevent the attacks from causing any harm. There is also the fact that the attacks are so small now that they would do little damage if they got through. This longevity issue presents us with a look at how state actors may come to use cyber warfare tactics in the future. State actors will have even greater resources with which to attack and so we can expect sustained attacks that will last for weeks, possibly even months. These attacks could cripple the economy of a nation and result in a loss of trust among the populace that would cascade through the system causing great damage financially. These organized attacks are also larger not just in time but in scope and can result in widespread failures that may take time to repair.

Conclusion

From my data analysis I have found a number of trends that will come to bear importance in understanding past cyber tactics and their future. Cyber tactics have been executed with and will most likely continue to be executed with a political motive. This stands in only partial support of my first hypothesis as most attacks were not hacktivist. On the matter of my second hypothesis though, we cannot say that the data is in any way conclusive. While a majority of attacks have been executed by non-state civilian activists this data cannot be considered the final judgment, because there was not sufficient data and because this trend seems like it could be changing. A number of attacks have been executed by criminal organizations and we have slowly seen the entrance of state actors into this arena. The recent establishment of CYBERCOM is a testament to this fact (Gorman & Dreazen, 2009). The third hypothesis regarding severity is strongly supported by the data as a majority of the attacks are not very damaging.

The relation between the increase in larger, longer, more severe attacks over time shows a dedication to increasingly complex and pre-meditated attacks. If this trend continues we will certainly hear more of DDoS in the future. This tendency to move towards attacks with a larger use of resources could see greater involvement of government agencies. The potential provided by a well-organized DDoS attack can prove to make it a very useful weapon of war. An attack by a country with the computing power of the United States could cause great harm to the network infrastructure of its enemies if they are not prepared for such an attack.

This research is just a start. The issue that still needs to be dealt with is a lack of data, specifically that related to actors. Some data just cannot be found because of the nature of DDoS attacks, and this affects the results in a number of ways. The only data that I can say is fully conclusive is that on targets and motive. As we move into the future it will become easier to trace DDoS attacks, this has already been seen with the conviction of individuals who were involved in the Estonian attacks (Nazario, DDoS Fines in Estonia 2008). Perhaps as this information becomes more accessible a much better job can be done of compiling and analyzing the data on cyberterrorism and cyber warfare. For the time being I hope that my research has provided a sufficient stepping stone in understanding the workings of cyberterrorism, and more specifically DDoS attacks.

While this research shows that the threat of attacks is not as high as some in government and the media have presented this does not mean that the threat should be ignored. Trends show an increasing use of cyber-tactics and it is more than likely they will also become more damaging. Currently the Internet has the infrastructure to sustain such attacks but everyday more and more people use the Internet while the amount of infrastructure being built cannot keep up with demand. Some have cited concerns that the Internet will soon suffer brownouts and blackouts like the electrical grid. If this is true then it will also be unable to sustain a massive DDoS attack. Government officials and military personnel must take heed of this concern as we move into an ever connected world. While terrorist organizations have yet to use DDoS tactics we cannot ignore the possibility that they may in the future. The threat posed by large criminal syndicates is also of concern. Ultimately I believe that DDoS will be used increasingly along with other tactics of cyber warfare to serve as support to physical attacks.

Works Cited

Barnes, Julian E. *Pentagon Computer Networks Attacked.* 28 November, 2008. http://articles.latimes.com/2008/nov/28/nation/na-cyberattack28.

BBC Monitoring Kiev Unit. "Belarusian web site accuses authorities of inspiring hackers' attacks." February 11, 2004.

BBC Worldwide Montoring. "Burma Government blamed for attack on website of exile radio, TV." July 25, 2009.

Borglund, Josh. *Top 5 Most Costly Viruses of All Time.* 2009. http://anti-virus-software-review.toptenreviews.com/top-5-most-costly-viruses-of-all-time.html.

Coleman, Kevin. *CYBER WAR 2.0 -- RUSSIA V. GEORGIA.* August 13, 2008. http://www.defensetech.org/archives/004363.html.

Collin, Barry C. *The Future of CyberTerrorism: Where the Physical and Virtual Worlds Converge.* February 2004. http://www.crime-research.org/library/terrorism02_2004.html.

Conway, Maura. "Cyberterrorism: Academic Perspectives." Edited by Andy Jones. *Proceedings of the 3rd European Conference on Information Warfare and Security*, 2004: 41-50.

Conway, Maura. "Cyberterrorism: Hype and Reality." (Dublin City University) 2007.

Conway, Maura. "Hackers as Terrorists? Why it Doesn't Compute." *Computer Fraud and Security* 203, no. 12 (December 2003): 10-13.

Conway, Maura. "Reality Bites: Cyberterrorism and Terrorist "Use" of the Internet." July 2002.

Cortes, Lieutenant Colonel Wanda I. "Cyber Terrorism Post 9/11 in the Western Hemisphere." *Fort Lesley J. McNair*, April 2004.

Crawford, H, and B Cronin. "Information warfare: its application in military and civilian contexts." *The Information Society* 15, no. 4 (1999): 257-63.

Danchev, Dancho. *Coordinated Russia vs Georgia cyber attack in progress.* August 11, 2008. http://blogs.zdnet.com/security/?p=1670.

Denning, Dorothy E. "Hacktivism and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy." In *Networks and Netwars: The Future of Terror, Crime, and Militancy*, edited by J Arquilla and DF Ronfeldt, 239-288. Rand, 1999.

Denning, Dorothy E. "Information Operations and Terrorism." In *Terrorism in the Information in the Information Age: Understanding the Threat of Cyber-Warfare*, edited by Lars Nicander and Magnus Ranstorp. Hurst, 2005.

Denning, Dorothy E. "Barriers to Entry." *IO Journal*, April 2009: 6-10.

—. "Cyberterrorism Testimony before the Special Oversight Panel on Terrorism, Committie on Armed Services, U.S House of Representatives." Washington, DC, May 23, 2000.

Epstein, Keith. *U.S. Is Losing Global Cyberwar, Commission Says.* December 7, 2008. http://www.businessweek.com/bwdaily/dnflash/content/dec2008/db2008127_817606.htm.

Freeh, Louis. "Statement for the Record on Cybercrime." *Senate Committee on Judiciary, Subcommittee for the Technology, Terrorism, and Government Information.* Washington, DC, March 28, 2000.

Furnell, S.M., and M.J. Warren. "Computer Hacking and Cyber Terrorism: The Real Threats in the New Millenium?" *Computers & Security*, no. 18 (1999): 28-34.

Goodin, Dan. *US teen admits to 'Anonymous' DDoS attack on Scientology.* October 17, 2008. http://www.theregister.co.uk/2008/10/17/scientology_ddos_guilty_plea/.

Gorman, Siobhan. *Electricity Grid in U.S. Penetrated By Spies* . April 8, 2009. http://online.wsj.com/article/SB123914805204099085.html#articleTabs%3Darticle.

Gorman, Siobhan, and Yochi J Dreazen. *New Military Command to Focus on Cybersecurity.* April 22, 2009. http://online.wsj.com/article/SB124035738674441033.html.

Goth, Greg. "The Politics of DDoS Attacks." *IEEE Distributed Systems Online* 8, no. 8 (August 2007).

Gralla, Preston. *CIA: Hackers have already attacked the electric grid.* March 26, 2009. http://www.greenercomputing.com/blog/2009/03/26/cia-hackers-have-already-attacked-electric-grid.

Halpin, Tony. *Putin Accused of Launching Cyber War.* May 18, 2007. http://www.timesonline.co.uk/tol/news/world/europe/article1805636.ece.

Haug, Laurent. *Bruce Sterling on Estonian Cyberwar.* September 20, 2007. http://liftlab.com/think/laurent/2007/09/20/bruce-sterling-on-the-estonian-cyberwar/.

Higgins, Kelly Jackson. "Botnets Wage Internecine War." *InformationWeek*, April 23, 2007: 35.

Ingram, Matthew. "How the Net beat a hack attack; Your computer may have helped a bid to bring down the Web but the Internet fought back." *The Globe and Mail (Canada)*, February 10, 2007: A10.

"Joint Publication 3-13.3: Operations Security." Joint Staff, n.d.

Jones, Dr. Andrew. "Cyber Terrorism: Fact or Fiction." *Computer Fraud and Security*, June 2005: 4-7.

Karatzogianni, Athina. "The Politics of "Cyberconflict"." 2002.

Kelly, John J, and Lauri Almann. "eWMDs." *Policy Review* (Hoover Institution), 2008-9.

Koman, Richard. *Massive Chinese spynet targeted Dalai Lama.* March 29, 2009. http://government.zdnet.com/?p=4498.

Landler, M, and J Markoff. *Digital Fears Emerge After Data Siege in Estonia.* May 29, 2007. http://www.nytimes.com/2007/05/29/technology/29estonia.html?pagewanted=1&ref=technology.

Lawson, Sean. "The Cyber-Intifada: Activism, Hactivism, and Cyber-Terrorism in the Context of the “New Terrorism”." Fall 2001.

Lewis, James A. *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats.* Washington, DC: Center for Strategic and International Studies, 2002.

Lewis, James A. *Securing Cyberspace for the 44th Presidency.* Washington, DC: Center for Strategic and International Studies, 2008, 90.

Lipschutz, Ronnie D. "Terror in the suites: Narratives of fear and teh political economy of danger." *Global Society* 13, no. 4 (1999): 411-39.

Macket, Robert. *Are "Cyber-Militias" Attackng Kyrgyzstan?* February 5, 2009. http://thelede.blogs.nytimes.com/2009/02/05/are-cyber-militias-attacking-kyrgyzstan/.

Markoff, John. *Before the Gunfire, Cyberattacks.* August 13, 2008. http://www.nytimes.com/2008/08/13/technology/13cyber.html?_r=2&hp&or ef=slogin.

—. *Defying Experts, Rogue Computer Code Still Lurks* . August 26, 2009. http://www.nytimes.com/2009/08/27/technology/27compute.html?_r=2&nl=technology&emc=techupdateema1.

McCarthy, Kieren. *Mafiaboy given eight months.* September 13, 2001. http://www.theregister.co.uk/2001/09/13/mafiaboy_given_eight_months/.

McMillan, Robert. *Cyberattacks on US military jump sharply in 2009.* November 20, 2009. http://www.pcworld.idg.com.au/article/327075.

Mills, Elinor. *Radio Free Europe DDOS attack latest by hacktivists.* May 1, 2008. http://news.cnet.com/8301-10784_3-9933746-7.html.

Mirkovic, Jelena, and Peter Reiher. "A Taxonomy of DDoS and DDoS Defense Mechanisms." *ACM SIGCOMM Computer Communication Review*, April 2004: 39-53.

Nagpal, Rohas. "Cyber Terrorism in the Context of Globalization." *II World Congress on Informatics and Law*. Madrid, Spain, 2002.

Naraine, Ryan, and Dancho Danchev. *Coordinated Russia vs Georgia cyber attack in progress.* August 11, 2008. http://blogs.zdnet.com/security/?p=1670.

Nazario, Jose. "DDoS Attack Evolution." *Network Security*, July 2008: 7-10.

—. *DDoS Fines in Estonia.* 2008 йил 23-January. http://asert.arbornetworks.com/2008/01/ddos-fines-in-estonia/.

—. *Estonian DDoS Attacks: A Summary to Date.* May 17, 2007. http://asert.arbornetworks.com/2007/05/estonian-ddos-attacks-a-summary-to-date/.

Nunn, Sam. "Get Ready for Cyberwar: Blueprint Magazine." *Progressive Policy Institute.* January 1, 2000. http://www.ppionline.org/ppi_ci.cfm?knlgAreaID=124&subsecID=160&contentID=1130.

Orlando, Carlo. *Obama Stimulus Pours Millions into Cyber Security.* March 2, 2009. http://www.infopackets.com/news/security/2009/20090302_obama_stimulus_pours_millions_into_cyber_security.htm.

Paxson, Vern. "An analysis of using reflectors for distributed denial-of-service attacks." *ACM SIGCOMM Computer Communication Review* 31, no. 3 (2001): 38*47.

Pincus, Walter. *Pentagon Official Warns of Risk of Cyber Attacks.* March 17, 2009. http://www.washingtonpost.com/wp-dyn/content/article/2009/03/17/AR2009031702715.html?nav=rss_email/components.

Pollitt, Mark M. "Cyberterrorism: Fact or Fancy?" *Computer Fraud and Security* 1998, no. 2 (1998): 8-10.

Poulsen, Kevin. *Botnets Beat Spartan Laser on Halo 3.* February 4, 2009. http://www.wired.com/threatlevel/2009/02/botnets-beat-sp/.

Report: Cyberspy network targets governments. March 29, 2009. http://www.cnn.com/2009/TECH/03/29/ghostnet.cyber.espionage/index.html?eref=rss_latest.

Report: White House should oversee cybersecurity. December 8, 2008. http://www.cnn.com/2008/TECH/12/08/cyber.security/index.html?eref=rss_latest.

Richtel, Matt. "Yahoo Blames a Hacker Attack for a Lengthy Service Failure." *The New York Times*, February 8, 2000: C11.

Ross, Jeffrey Ian. "Structural Causes of Oppositional Political Terrorism: Towards a Causal Model." *Journal of Peace Research* 30, no. 3 (1993): 317-329.

Rubin, Courtney. *Report Says Google Attack Traced to Two Chinese Schools.* 2 19, 2010. http://www.inc.com/news/articles/2010/02/google-attack-traced-to-2-chinese-schools.html.

Shachtman, Noah. *Top Georgian Official: Moscow Cyber Attacked US-We Just Can't Prove It.* March 11, 2009. http://www.wired.com/dangerroom/2009/03/georgia-blames/.

—. *Web Attacks Expand in Iran's Cyber Battle.* June 16, 2009. http://www.wired.com/dangerroom/2009/06/web-attacks-expand-in-irans-cyber-battle/.

Swaine, Jon. *Georgia: Russia 'conducting cyber war'.* August 11, 2008. http://www.telegraph.co.uk/news/worldnews/europe/georgia/2539157/Georgia-Russia-conducting-cyber-war.html.

Tabatadze, Kate. *Cyber War: Russia vs Georgia.* August 11, 2008. http://www.fresnoundercurrent.net/node/1867.

Traynor, Ian. *Russia Accused of Unleashing Cyberwar to Disable Estonia.* May 17, 2007. http://www.guardian.co.uk/world/2007/may/17/topstories3.russia.

Vamosi, Robert. *First Conviction for Estonia's 'Cyberwar'.* January 24, 2008. http://news.cnet.com/8301-10789_3-9857492-57.html.

Weimann, Gabriel. *Cyberterrorism: How Real is the Threat?* Washington, DC: United States Institute of Peace, 2004, 12.

—. *Terror on the Internet: The New Arena, The New Challenges.* Washington DC: United States Institute of Peace Press, 2006.

Wilson, Clay. *Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress.* Washington, DC: Congressional Research Service, 2008, 40.

Wilson, Clay. *Information Operations, Electronic Warfare, and Cyberwar: Capabilities and Related Policy Issues.* Washington, DC: Congressional Research Service, 2007, 16.