Cyber Warfare: The Newest Battlefield

Chad Nelson, chad.nelson@wustl.edu (A project report written under the guidance of Prof. Raj Jain) Download

Abstract

Today's world is becoming increasingly dependent on computers and increasingly connected through the Internet. These two facts have created a new battlefield for countries to wage war on. Using various methods of cyber attacks, depending on the situation, an aggressor country can cripple or demoralize its target without using any military force and can do so with almost total anonymity. If combined with a traditional military force, a successful cyber attack can prevent an enemy from mounting an effective defense, making the military action more likely to succeed with fewer casualties. No country has yet admitted to organizing a cyber attack, but it is likely that at least one country has successfully launched a cyber attack in such a way that it can't be proved. In the near future, cyber warfare will become more popular to antagonize other countries, but will never be used openly due to the possibility of mutually assured destruction.

Table of Contents

1. Introduction

Recent advances in technology have completely changed how we live on this planet. Everything can be done in an online world now, from shopping to banking to collaborating on projects. As with all technologic advances in history, this cyber world has also been turned into a weapon. It began with individuals pushing the limit of the web or going for personal gain, but now governments have begun to realize that the potential for a cyber attack is very real, and the resulting damage could be catastrophic. Because of this, several countries are researching and preparing cyber defenses, independently and collaboratively.

At the same time, being able to organize such an attack would allow a nation to cripple an enemy without any traditional military action. This has prompted governments to also invest in cyber weapons. Because of the Internet's anonymity, it is easy for an attacker to either hide his tracks or leave a false trail. As such, there have been several large cyber attacks already that cannot be definitively traced to a country, organization, or person. Only the motives behind the attack and how the attack was performed can give clues towards the aggressor.

2. Methods of Attack

There are many ways to attack a computer or network of computers. In cyber warfare, the method chosen is based on what the attacker's goals are. For example, a nation may want to snoop through a rival's bank system to look for economic instability one month, then crash it the next month to cause economic instability. The ubiquity of computers basically guarantees that whatever an aggressor want to do to a target, he can do, as long as he uses the right attack and has an intelligent group of people to organize it.

2.1 Malware

All computer users know that malware is bad. However, many users aren't good at avoiding malware. Because governments employ many people, chances are good that at some point, some government computer will get infected. What happens after that depends on what it was infected with.

For example, in mid-2009 a virus known now as Stuxnet began to infect computers around the globe. Symantec, an antivirus corporation, noticed and cataloged it, but it didn't get much attention because it wasn't causing any problems. A small security company in Germany began investigating it and found out the virus would only cause problems in very specific circumstances. Ralph Langner, the owner of the security firm, said "It was a marksman's job" [Broad11]. A few months later, the virus struck. Nearly 1000 machines responsible for enriching uranium in Iran were destroyed.

Enriched uranium can be used to create nuclear weapons, and the destruction of the equipment caused a major setback in Iran's nuclear program. Stuxnet appears to have been targeted at that equipment. When it was on the computers responsible for those machines, it first waited and gathered data from the normal operations. Then, it caused the machines to lose control and destroy themselves while reporting that everything was fine. Stuxnet has been called the "most advanced cyberweapon ever deployed" [Broad11].

Langner also reported that "anyone who looks at it carefully can build something like it" [Broad11]. In late 2011, it turned out someone had. A new virus, DuQu, was found by Symantec. At first it was classified as Stuxnet, but they realized it was something else. Stuxnet just used other computers as a way to get to its target. DuQu, however, was gathering information on every computer it infected. It stayed on each computer 36 days profiling the computer and the network and keeping a log of all keystrokes. It sent all this information off to a secure server, and when its time was up in removed itself. Because it was just discovered, no one knows how many computers it has gathered information on or what the information will be used for. However, it is likely that it was gathering information in preparation for some sort of attack [Rash11].

2.2 Denial of Service

A denial of service attack, or DoS attack, is a method of attack that aims to disable a server or network by flooding it with messages. If the attack is successful, the target will be unable to deal with all of the incoming traffic. The target will then most likely crash or reboot. Depending on how the system is set up, this may in turn cause damage to the server or applications running on it. The main goal of a DoS attack, however, is in its name; it denies legitimate users access to the system [McDowell09].

This makes it a fantastic propaganda tool. Average users wouldn't have any idea what's actually going on; all they know is the site or service they wish to use won't respond. They realize there's something wrong with the system, and they lose confidence in it. Such an attack can cost a company millions in lost revenue during the outage, plus the cost to repair damage and the loss of users in the long term [McDowell09].

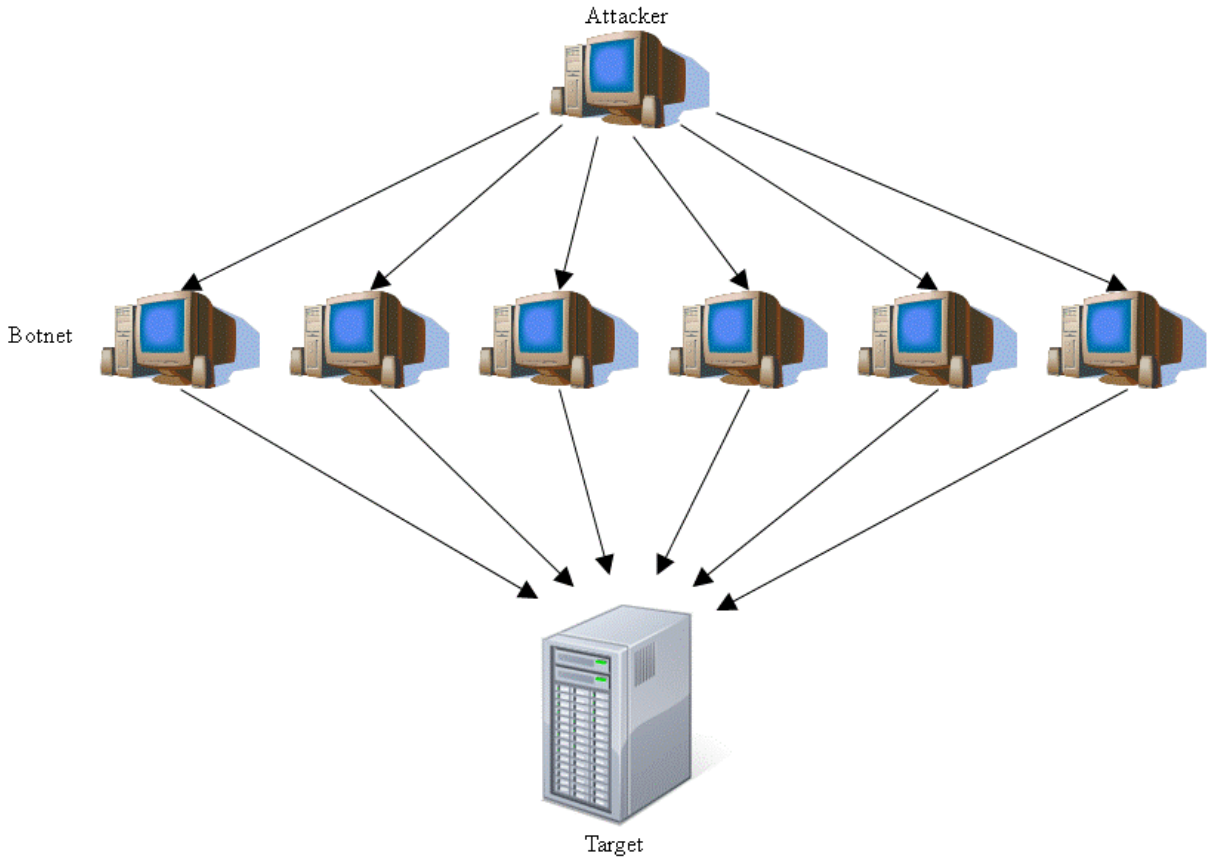
When used in warfare, the effects of a DoS attack can be even more dangerous. Because people are so used to having access to lots of information at all times, an attack on a government or news site can cause panic. The effect is multiplied if the attack is done during a time of turmoil, such as during an aggressive military action or civil unrest. Furthermore, the citizens of the afflicted country may turn to other sources for information, giving the aggressor an opportunity to spread its propaganda. If government or military communications centers are attacked, the target country's leadership will be unable to coordinate to figure out what is happening. This lack of response will cause even more fear amongst the population and within the government [Karia10].

2.3 Variations of DoS Attacks

In a traditional DoS attack, an attacker uses a single machine to repeatedly send messages to a target, using up its bandwidth and completing the attack. However, this is no longer practical for several reasons. First, most large servers and any worthy cyber warfare target would have a large enough bandwidth to handle a single machine, unless it was another large server. This is generally not the case, so in most cases the target would actually be able to handle the attack, even if its service is somewhat slowed for the duration. Second, most servers only allow a certain number of requests in a given time period from a single machine. This means the attacker would soon start to have his messages rejected, defeating the attack. Finally, the attackers IP address would be well-documented after the attack and easy to track down.

Single machine DoS attacks are no longer used because of these weaknesses. Today, the most popular form of DoS is a distributed denial of service attack, or DDoS. Figure 1 shows an example of a DDoS attack.

Figure 1 DDoS attack



Attacker sends command to botnet, botnet floods server with messages

The principle is the same as a traditional DoS attack. However, instead of a single computer, hundreds or thousands of computers are used. These are often privately owned computers infected with a virus, so tracing them to the attacker is impossible. Because there are so many, the target cannot block them all before crashing. Some people in cyber crime make their living by controlling large botnets, which are collections of infected computers ready to flood a target whenever the command comes in. Botnets can often be rented for pennies per computer [Markoff08], making them a cheap and effective way to disrupt a nation's communication and cause unrest in the population [McDowell09].

The only problem a government would run into while using a DDoS attack is how to get a botnet. If a government tried to create its own botnet and was discovered, it would be in serious trouble with its citizens and the rest of the world. If it rents from a cyber criminal, the attack may be traced back to the country that ordered it if the cyber criminal doesn't keep quiet. However, governments with the means and motive to hire a botnet will probably be able to cover their tracks. As such, there have already been DDoS attacks allegedly linked to a country, but without solid proof.

Another form of DoS attack is a permanent denial of service attack, or PDoS. This attack is specifically designed to damage the target's hardware, rather than just crash or deny access. It does this by corrupting the target's firmware. After this, the hardware must either be flashed with new firmware or replaced. Either way, the targeted system is taken down for a long period of time after a quick connection. This attack would only work on devices that can be flashed over a network: most likely an unsecure router or switch. There have been no known PDoS attacks outside of research settings, possibly due to the limitation on what systems can be attacked [Higgins08].

3. Methods of Defense

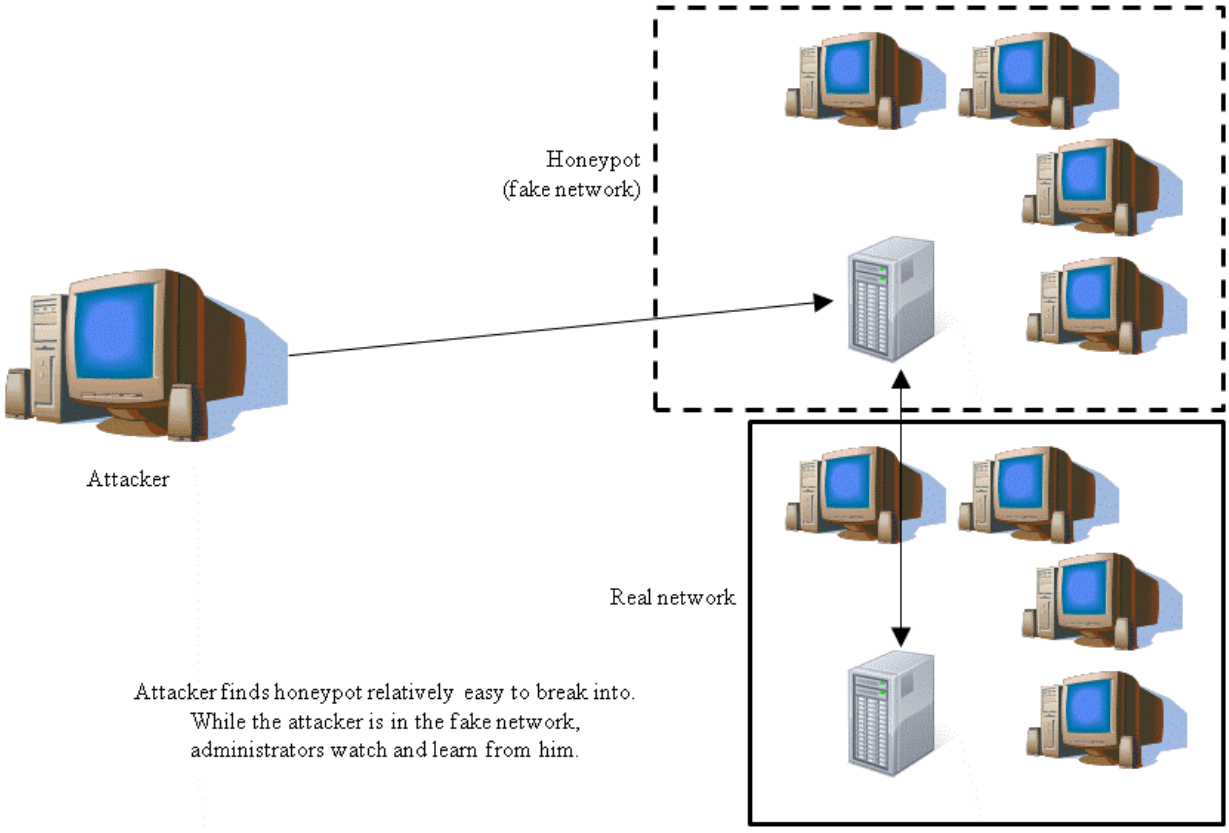
In 2009, the Pentagon announced that it had spent over $100 million to repair damage done by cyber attacks over a 6 month period [Hasson09]. That doesn't include research done to prevent future attacks. With that much money going into keeping its systems in working order, the Pentagon has recently decided to switch its defensive strategy. More specifically, it plans to move from passive defenses to passive and active defenses. To understand what this means, it's important to understand what passive and active defenses are in the cyber world.

3.1 Active Defenses

Active defenses take action to prevent or retaliate when the system is attacked. The Pentagon describes it as introducing military concepts such as organizing, training, and equipping its personnel and using strategy to defend its cyber resources [Alexander11]. One form of active defense is called a honeypot. With a honeypot a fake network is created and attached to the network that is being protected. Some security holes are left open, but it's

kept secure enough to make the attacker think it's a network that's in use. The administrators can then track the attacker and his actions. From this, they can often tell what the attacker is after and how skilled the attacker is. If the attacker is particularly careless, it may be possible to trace him and find him [McGrew06]. This opens up the possibility of retaliating against the attacker. Figure 2 shows a simple example of a honeypot.

Figure 2 Honeypot



Because DDoS attacks are so easy to perform and can cause huge problems, there has been a lot of research into preventing a DDoS attack from taking down the target. This is a difficult task, as the goal of DDoS is to overload the system. If the attack gets that far, the target may not be able to call for help or have the resources to deal with the attack. So, prevention is the best way to deal with it. DDoS can be prevented by carefully filtering packets before sending them to the server. If a router can recognize that it's getting a lot of the same message from the same place, it should not transmit them to the server. Also, a firewall can be installed that only allows network traffic on approved ports. This is still vulnerable, but not as vulnerable as system with all ports open [Srivastava11].

In some systems, a DDoS attack can be detected and mitigated so that the server withstands the attack and stays online. There are two general ways to detect a DDoS attack. The first is based on previous knowledge of what DDoS attack looks like. If the same signature occurs, it means the system is probably under attack. The second creates a profile of normal activity. If activity deviates from that profile, the system may be under attack. Using the second method, anomaly based detection, can detect previously unseen attacks, but also generally result in more false alarms [Srivastava11].

3.2 Passive Defenses

Passive defenses don't search for problems on the computer. Instead, they try to prevent the computer from being attacked in the first place. Examples include firewalls, antivirus software, and access control. Firewalls monitor incoming connections and deny those it deems dangerous or untrustworthy. Antivirus software can scan the files that are allowed through to be sure they aren't hiding malicious code. Finally, access control assigns users and computers to different permission categories. This can prevent a compromised computer or user account from damaging the entire network. Most companies have some form of each of these implemented on their network or computers.

There are a number of problems with this approach to security. First, each of these security measures reduces usability as it increases security. The most secure system would allow for no input, but it would be totally useless, while an entirely open system would be user-friendly but infected in minutes. Second, an attacker only needs to find one point of entry to compromise the system. From there he can often turn off the other defenses (with the exception of access control). Points of entry can come from user error or flaws in the security programs. This requires an unending series of patches and updates along with repairs, which cost a lot of time and money.

4. Current World Affairs and Cyber Warfare

As with any warfare, cyber warfare can be a key issue in international politics. However, unlike traditional warfare, cyber warfare makes it difficult, if not impossible, to know who the attacker is. Even if an attack can be traced back to its origin, it doesn't mean that country was behind the attack. Because of this, there has been an arms race to get a fully operational cyber division in several countries that is prepared to either mount a cyber attack or defend against one. This is confirmed by McAfee, which reported an increase in government-based cyber warfare [Brodkin07]. The major world players in the cyber arena so far have been the United States, China, Russia, and North Korea.

4.1 United States

In February of 2010, the United States launched Cyber ShockWave, a cyber war game to see how the nation would be able to respond after a serious cyber attack. The result showed that the US was not well-prepared for such an attack [Chertoff10]. A number of things need to be done to get the country up to par. First, it needs to be clearly stated what powers the government has in this state of emergency. Second, there needs to be some policy in place that state how much control over the Internet and privacy the government would have. Third, a system must be developed that allows public and private security experts to work together during the attack. Finally, a policy must be drawn up that outlines how the US would respond if attacked by another nation. This would also serve as a deterrent from mounting a cyber attack on the US [Chertoff10]. Also, malware has been found in the US electrical grid that could allow the attackers who put it there to interfere with the system [Gorman09]. This suggests that attacks may already be coming or are coming soon. Some analysts report that the US is so vulnerable to cyber attack that it should be viewed a deterrent against going to war. The reasoning is that if the US tries to attack a country, it will retaliate with cyber attacks that cripple the US electricity grid, banking, or other vital services [Baldor11].

Because US Cyber Command is part of the military, some people are worried about the militarization of the Internet. However, the US has never officially launched a cyber attack. The US did almost use cyber attacks before going into Libya [Wagenseil11]. Officials have said they don't want to set a precedent by being the first to openly use cyber warfare, and it's better to keep the US's capabilities secret for as long as possible. There is evidence, however, that the United States and Israel were behind the Stuxnet attack on Iran as an attempt to slow down Iran's nuclear program [Broad11].

4.2 China

China is a perfect example of how difficult it is to say exactly who is behind a cyber attack. In December of 2009, 34 US companies were victims of cyber attacks. One of these was Google, who reported that the Gmail accounts of Chinese human rights advocates in China, Europe, and the US were hacked into. The other targeted companies happened to specialize in areas that the US is doing much better than China, suggesting that the attacks may have been to steal information [Weldon10]. Even with all of this information, it is impossible to say for sure that China is behind the attacks because it may be the case where someone is trying to antagonize China-US relations. Google was convinced China was behind the attack and threatened to pull its operations out of China. Google ended up staying in China, but this shows that a private company may have more sway that a country on the cyber battlefront.

4.3 Russia

In 2007, Estonia decided to move a Soviet World War II era monument from its capital. This was met with stiff resistance from the Russians in Estonia as well as from Russia itself. In response, Russians in Estonia began protesting. Then, Estonia became the first country to be the victim of a coordinated cyber attack. It started slowly, but ended up taking down the government websites and banking sites. The loss of banking was especially bad because about 97 percent of Estonia's banking takes place online [Richards07]. This also took down Estonia's ATM system and prevented Estonians from withdrawing money outside of Estonia, as well. News and media outlets were attacked, too. Eventually, the government cut Estonia off from the rest of the Internet to stop the attacks, which allowed the country to recover and re-establish internal connections. While it appears obvious that Russia was behind the attacks, the Russian government denied all involvement, and of course it can't be proved one way or the other.

In 2008, Russia was involved in a 10 day war in Georgia. 3 days before Russia took military action, there was an attack on Georgia's networks. The government sites were either defaced or hit with a DDoS attack, news, media, and financial institutions were attacked with DDoS, and malware was uploaded onto Georgian websites. This marks the first time that a cyber attack coincided with traditional military action [Tikk08].

4.4 North Korea

North Korea is in an ideal position for cyber offense. The nation itself has limited Internet access due to Kim Jon Il restricting its use, making it a weak target. However, North Korea neighbors the country with the best Internet connectivity; 95 percent of South Korea has high-speed Internet access [Harlan11]. So, if the North Koreans can connect to a computer in South Korea, from there they have a high speed connection to almost anywhere. In April of 2011, half of the servers owned by a South Korean bank crashed, and evidence pointed to North Korea. Again, North Korea denies these accusations, but most countries don't believe that. Now, there is some worry that they will escalate to South Korean military targets and get military secrets of South Korea or its allies. Some South Korean military networks had been compromised in the past, but their security has been upgraded [Harlan11].

Kim Heung-kwang is a former North Korean computer science professor who defected to South Korea. Kim says that in North Korea, elementary students who excel at math are identified and prepared for cyber warfare from that early age. At the university level, they are trained at specific institutions in North Korea, and then they study in either China or Russia for additional training. This system produces around 50 new recruits every year for North Korea's cyber warfare division, Unit 121. However, this information has not been verified by another source [Harlan11].

5. International Collaboration

With such power and anonymity behind cyber attacks, the best way for nations to defend themselves is to work together. After the attacks on Estonia in 2007, NATO (North Atlantic Treaty Organization) decided to establish a cyber defense center. The Cooperative Cyber Defence Center of Excellence was established in Estonia to research cyber warfare attacks and cyber defenses [McMillan08]. In June of 2011, NATO established the NATO Policy on Cyber Defence. This policy contained several important parts. First, it requires that all NATO structures must be brought under centralized protection with new security rules. It also states how NATO will response to cyber threats and how NATO will assist its members if they request assistance in setting up cyber defense. Finally, the policy states how NATO will cooperate with members, international organizations, private entities, and academia [NATO11]. The goal is to share as much information as possible and build upon it so everyone involved can be as protected as possible. Such a large scale effort to defend against cyber attacks would be difficult for a single country to fund and maintain, but a collection of countries working together can do it successfully.

6. Conclusion

Cyber attacks are going to continue. They are cheap, near-anonymous, and can be very effective. When used alongside military action, propaganda, or civil unrest, the effect multiplies; people used to their computer services don't like to lose them. With the Internet linking up almost every computer, important infrastructure and government computers are at risk as well. In most developed nations, the consequences of a cyber attack can be so great that the threat of an attack may be able to deter military or political action. Because of this, governments and private citizens and companies have started working together to implement active cyber defenses. With this collaboration, the Internet will hopefully remain safe for everyone.

References

1. [Broad11] Broad, William J., Markoff, John, and Sanger, David E. "Israeli Test on Worm Called Crucial in Iran Nuclear Delay," The New York Times. January 15, 2011. p. 1-4 http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html
2. [McDowell09] McDowell, Mindi. "Understanding Denial-of-Service Attacks," US-CERT. November 4, 2009. http://www.us-cert.gov/cas/tips/ST04-015.html
3. [Harlan11] Harlan, Chico; Nakashima, Ellen. "Suspected North Korean Cyberattack on a Bank Raises Fears for S. Korea, Allies," Washington Post. p. 1, 2. August 20, 2011. http://www.washingtonpost.com/world/national-security/suspected-north-korean-cyber-attack-on-a-bank-raises-fears-for-s-korea-allies/2011/08/07/gIQAvWwIoJ_story.html
4. [Srivastava11]A. Srivastava, B. B. Gupta, A. Tyagi, Anupama Sharma, and Anupama Mishra. "A Recent Survey on DDoS Attacks and Defense Mechanisms," Advances In Parallel Distributed Computing. 2011. p. 575, 576. http://www.springerlink.com/content/j21621tm87v24340/
5. [Chertoff10] Chertoff, Michael. "Cyber ShockWave Exposed Missing Links in U.S. Security," Government Computer News. p. 1, 2. March 10, 2010 http://gcn.com/Articles/2010/03/15/Commentary-Chertoff-Cyber-ShockWave.aspx
6. [Karia10] Karia, Jiten. "How DDoS attacks became the frontline tool of cyber-war," The Next Web. December 19, 2010. http://thenextweb.com/media/2010/12/19/how-ddos-attacks-became-the-frontline-tool-of-cyber-war/
7. [Markoff08] Markoff, John. "Before the Gunfire, Cyberattacks," The New York Times. August 12, 2008. http://www.nytimes.com/2008/08/13/technology/13cyber.html
8. [Higgins08] Higgins, Kelly J. "Permanent Denial-of-Service Attack Sabotages Hardware," Dark Reading. May 19, 2008. http://www.darkreading.com/security/client-security/211201088/permanent-denial-of-service-attack-sabotages-hardwar
9. [Rash11] Rash, Wayne. "DuQu Worm Causing Collateral Damage in a Silent Cyber-War," eWeek. November 2, 2011 http://www.eweek.com/c/a/Security/Duqu-Worm-Causing-Collateral-Damage-in-a-Silent-CyberWar-782686/
10. [Hasson09] Hasson, Judi. "DoD spent $100M to fix cyber attack damages," FierceGovernmentIT. April 8, 2009. http://www.fiercegovernmentit.com/story/dod-spent-100m-fix-cyber-attack-damages/2009-04-08
11. [Alexander11] Alexander, David. "Pentagon Tries to Lean Forward in Cyberdefense," AviationWeek. July 14, 2011. http://www.aviationweek.com/aw/generic/story_channel.jsp?channel=defense&id=news/awx/2011/07/14/awx_07_14_2011
12. [McGrew06]McGrew, Robert; Vaughn, Rayford B., Jr. "Experiences With Honeypot Systems: Development, Deployment, and Analysis," IEEEXplore. p. 5, 6. 2006. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1579742
13. [Brodkin07] Jon Brodkin. "Government-sponsored Cyberattacks on the Rise, McAfee says," Network World. p. 1 http://www.networkworld.com/news/2007/112907-government-cyberattacks.html
14. [Gorman09] Gorman, Siobhan. "Electricity Grid in U.S. Penetrated By Spies," Wall Street Journal. p. 1. April 9, 2009. http://online.wsj.com/article/SB123914805204099085.html
15. [Wagenseil11] Wagenseil, Paul. "U.S. Reportedly Considered Cyberattack on Gadhafi," Security News Daily. p. 1 October 17, 2011. http://www.securitynewsdaily.com/obama-gadhafi-cyberwar-1247/
16. [Baldor11] Baldor, Lolita C. "Cyber Weaknesses Should Deter US From Waging War," MSNBC. p. 1. November 7, 2011. http://www.msnbc.msn.com/id/45199096/ns/technology_and_science-security/t/cyber-weaknesses-should-deter-us-wagin
17. [Weldon10] Weldon, Owen. "Google China Cyberattack Part of Vast Espionage Campaign," p. 1. January 13, 2010. http://digitaljournal.com/article/285641
18. [Richards07] Richards, Jason. "Denial-of-Service: The Estonian Cyberwar and Its Implications for U.S. National Security," p. 1. 2007. http://www.iar-gwu.org/node/65
19. [Tikk08] Tikk, Eneken; Kaska, Kadri; Runnimeri, Kristel; Kert, Mari; Taliharm, Anna-Maria; Vihu, Liis. "Cyber Attacks Against Georgia: Legal Lessons Identified," Cooperative Cyber Defence Centre of Excellence. p. 7-13. November 2008. http://www.carlisle.army.mil/DIME/documents/Georgia%201%200.pdf
20. [McMillan08] McMillan, Robert. "NATO To Set Up Cyber Warfare Center," Network World. p. 1. May 14, 2008. http://www.networkworld.com/news/2008/051508-nato-to-set-up-cyber.html

21. [NATO11] "NATO and Cyber Defence," North Atlantic Treaty Organization. p. 1. September 16, 2011. http://www.nato.int/cps/en/SID-70CBB31B-8D6C1F24/natolive/topics_78170.htm?

List of Acronyms

DoS	Denial of service
DDoS	Distributed denial of service
NATO	North Atlantic Treaty Organization
PDoS	Permanent denial of service

Last Modified: November 27, 2011.