https://doi.org/10.48009/1_iis_2020_290-300
Issues in Information Systems
Volume 21, Issue 1, pp. 290-300, 2020

CYBERWAR: FORMS AND EFFECTS

Dr. Roger Finnegan, University of the Cumberlands, roger.finnegn@ucumberlands.edu

ABSTRACT

Cyberwar is an attack on a country's information resources. It can take many forms including standalone Internet attacks and cyber-attacks combined with conventional attacks. The goals of a cyberwar can be to force surrender, create confusion and mistrust or create a false impression of the attacker. This paper examines recent developments in Estonia, where Russia waged a cyberwar against the country, as a model of a cyberwar. The Chiapas rebellion in Mexico is examined as a model of information warfare. The question as to whether the United States is currently involved in a cyberwar is also examined. The conclusion reached is that while not in a hot cyberwar the United States could be in a cyber cold war.

Keywords: Information Technology (IT), cyberwar, war, security, cybersecurity

INTRODUCTION

Cyberwar is warfare in cyberspace that entails the attack by an adversary on a country's information resources both physical and virtual. These attacks can be comprised of distributed denial of service attaches, computer network hacking and other security threats (Delio, 2001). A cyberwar or "cyber cold war" (Griffiths, 2007, para 1) could have a negative impact on a society's economy and governance.

Cyberwar will be studied from various perspectives. The different ways that researchers have of defining what cyberwar is will be explored. The current literature on cyberwar will be review as well as the existing thinking, research and theories on cyberwar from institutions such as the Rand Corporation and the U.S. Department of Defense. Also several books and a multitude of news stories that have been published on the subject in the past several years will be examined. This research will also seek to determine whether the United States is currently engaged in a cyberwar.

The forms of cyberwar will also be analyzed and discussed. The types of attacks that would be part of cyberwar will be explored. There are various scenarios for how a cyberwar could be carried out that include direct attack on the physical infrastructure, virtual attacks in cyberspace or a combination of the two (Kirk, 2003). Cyber-attacks that have already taken place, such the attack on Estonia, and attacks that may still be going on, such as attacks on Taiwan and the Pentagon will also be researched.

This research will examine the principles and operations of cyberwar as well as the various strategies of a cyberwar. The aims of the attackers and how they would go about prosecuting the war will also be analyzed. Security threats from cyber war will be examined as well as the types of coercion against societies, governments, corporations and individuals that could take place in a cyberwar. The effects of cyber war also will be examined including the possible social and political changes that could take place due to a cyberwar. The effects on personal freedoms and social mores will also be explored.

Specifically this paper will examine the questions of what is cyberwar? What are the types of cyberwar? What are the impacts of cyberwar?

Cyberwar

Cyberwar is, as the name implies, war in cyberspace. It is also known as cyber-warfare, cybernetic war (Post, 1979) and third wave war (Dearth & Williamson, 1996) and is related to information warfare and network-centric warfare. In its purest form it is a war against the adversary's information infrastructure. It is "war over the Internet" and "would be something that maliciously, directly cripples a country's ability to function" (Jackson, 2007, para. 2). The

great information superhighway, like the Roman roads and the German autobahn in past conflicts, provides the means for military capabilities to be moved quickly and effectively.

One of the main concepts of cyberwar is the idea of "achieving military objectives with an absolute minimum of force application and/or cost" (Dearth & Williamson, 1996, p. 23). Anything "that touches digital networks quickly feels the effect of falling costs" (Anderson, 2008, p. 144). This minimum and diminishing cost means that a country of any size can be involved in a cyberwar. It also means that cyberwars do not necessarily need to be fought between countries. Terrorist groups or organized crime syndicates could be the perpetrators of a cyberwar (McAfee, 2007). "Information warfare specialists at the Pentagon estimate that a properly prepared and well-coordinated attack by fewer than 30 computer virtuosos strategically located around the world, with a budget of less than $10 million, could bring the United States to its knees" (Webster & de Borchgrave, 1998, p. 2). This means that a small group of people have the capability of waging a cyberwar with a super-power and win.

Cyberwars will aim to "disrupt or damage what a target population knows or thinks it knows about itself and the world around it" (Arquilla & Ronfelt, 1993, para 8). The information that a people have about themselves or others will be the very thing attacked in such a war. A cyberwar will target the information and the communications systems that the information relies upon. As societies and economies become more information dependent, that dependency can be the area that will be exploited in a cyberwar (Rowan, 2001).

Cyberwarfare involves the virtual conducting of military functions with the goal of "achieving advantages over a competing nation-state or preventing a competing nation-state from achieving advantages over them" (Brenner, 2007, p. 401). Cybercrime, criminal acts perpetrated over the Internet, and cyberterrorism, terroristic actions accomplished via the Internet, can be part of a cyberwar but they do not have to involve countries. Cybercrime and cyberterrorism can be instigated by individuals and by small groups of individuals and not by countries or nations. Because of the anonymous nature of the Internet it is possible for attacks to be instigated and the origin of the attackers to be unknown (Brenner, 2007).

In cyberwar the soldier would be able to operate "in the infosphere, the virtual world where commerce, conversation and connectivity will all occur" (Adams, 1998, p. 14). The warrior would be able to insert viruses, read emails, hack networks and attack systems from anywhere in the world. The soldiers could be comfortably sitting, not on a battlefield, but at home in bed working on their computer. They could work nine to five and have weekends off. All of this while fighting a war. It is possible because it is a cyberwar.

"The mission of the United States Air Force is to deliver sovereign options for the defense of the United States of America and its global interests -- to fly and fight in Air, Space, and Cyberspace" ("Air Force mission statement, "2005, para 5). The US Air force has recognized the need to be prepared to defend the country in cyberspace and has added it to its mission statement. The Air Force also created a cyber command specifically to prepare and fight cyberwars.

Estonia

On April 26, 2007 Russia launched "the first full-blown cyber assault resembling an act of war" (Grant, 2008, p. 24) or "first Internet war" (Evron, 2007, p. 34) against the neighboring country of Estonia which had been part of the former Soviet Union. The government of Estonia had recently decided to relocate a war monument dedicated to the Red Army that was left over from the Soviet era. The assumption is that the cyber-attacks against Estonia were in retaliation for this decision (Aaviksoo, 2008, p. 28). The civilian ISPs were the first major part of the infrastructure that was attacked. Cutting the civilian population's link to the Internet caused the infrastructure to falter. The banking industry was another major part of the country that was attacked. Without the banks no economic transactions could be processed. News organizations were another part of the country that was attacked. This part of the attacked showed the importance of online news to the populous (Evron, 2007).

To thwart these attacks IT professions from all three areas worked together and shared information. The attacks were aimed at the Estonian economy and populous. The intent of the attacks was to cut the population off from the rest of the world and from each other. With the ISPs knocked out, email and IM communication were not possible. People have grown more dependent on the Internet for communication and without it they were silenced and

isolated. The attack on the banking system caused havoc with the economy. Even simple transactions for gasoline or food were disrupted without the banks. This part of the attack was aimed at bringing more misery to the populous. The attack on the online news organizations removed the ability of people to find out what was happening in their country. These losses of a source for information lead to confusion and more isolation (Evron, 2007).

The cyber-attack on Estonia is the model of what a cyberwar would be like. The attackers may not directly take on the military or government infrastructures since those would already be hardened against attacks. The attackers would look for soft targets such as those attacked in Estonia. If people could not communicate with each other, nor be informed from the news media about what was going on they will feel isolated and frightened. At the same time if they could not get money from ATM machines or use debit cards to buy necessities the population will grow hungry. This could lead to panic and social unrest. The attacker does not have to risk mounting a physical attacked to harm the citizens of its adversary. It can be done from thousands of miles away (Evron, 2007).

Taiwan-China

The ever-growing dependence on computer systems by the economic, political and social infrastructures of both China and Taiwan make both countries vulnerable to cyber-attacks. The two countries are in a cyber arms race that is part of their overall conflict. In this conflict Taiwan is thought to have the upper hand technologically. Cyberwar can shatter the boundaries between war and peace since the war can rage without outward signs. While conflict between the two countries is still at the propaganda stage, the struggle between Taiwan and China could rage silently while battles are being won and lost without any physical signs of destruction.

Cyber-attacks can be part of ongoing military operations that can come before, after or during conventional attacks (Rawnsley, 2005). Also, part of the threat of cyberwar is the ability to change the essential character of a society. The threat to Taiwan is that "computer-based information warfare that deliberately targets an enemy's political, economic, social and military infrastructures creates the possibility of a national crisis, in which Taiwan may then be exposed to attack from more conventional sources" (Rawnsley, 2005, p. 1064). Security is "socially constructed, and in particular is inseparable from the creation of identity" (Rawnsley, 2005, p. 1065).

The propaganda exchanges between Taiwan and China constitute a type of cyberwarfare. The attempt by each side to assume the role of victim to the other's aggression provides the provocation to continue the attacks. It also creates an atmosphere where the private citizen feels that they must also be part of the prosecution of the war by hacking and committing other forms of cyber-attacks. Also, with computer systems, it has become easier to determine the effects of any type propaganda or psychological warfare. An adversary can use a type of propaganda and gauge the reaction in real time. With that information the attacker can continue to adjust and focus the propaganda to get the desired results (Rawnsley, 2005).

Military thinkers call this type of war 4GW (fourth generation warfare). "Victory in 4GW warfare is won in the moral sphere. The aim of 4GW is to destroy the moral bonds that allows (sic) the organic whole to exist – cohesion" (Robb, 2004, para. 7). To do this the enemy must create menace, mistrust and uncertainty. The foe must threaten survival, increase the division between different groups, and disrupt the economy as well as people's belief in the future (Robb, 2004).

Moonlight Maze

Moonlight Maze is the codename for an operation that the Russian Federation allegedly launched to attack computer systems in the United States. The aim of the operation was not to shut the systems down but to take as much information from them as was possible (US Senate, 2000). The attacks lasted for at least three years and targeted sensitive, but not classified, information. The attacks illustrated weaknesses in the US defenses against such attacks (Abreu, 2001). The systems probed included those belonging to the Pentagon, NASA, the Energy Department, and universities, and labs where research was being done. The documents searched include designs of military technology, military base maps and information on troop strength (Kirk, 2003).

Cyberwar is war that is being waged across the Internet. The attacks on Estonia by Russia and the propaganda exchanges between China and Taiwan show that cyberwar is real and is already taking place. The attack on Estonia seemed to be launched to punish the country for a perceived insult. The China-Taiwan exchanges could be construed as the opening moves that could escalate into an all-out conflict that could be a cyberwar and a conventional war. The threat of cyberwar is real and both conflicts show ways in which it can be waged.

ANALYSIS

Forms of Cyberwar

Cyberwar can take on different forms. The forms of attack can depend upon the adversary who is launching the attack, their aim for the attack and the overall strategy for the cyberwar. Some adversaries may not want to risk a direct conventional attack but are willing to attack using the anonymity that the Internet provides. The attacker may not want to dominate and defeat their victim but only punish or frighten them. The motivation for the cyberwar could be as straight forward as greed with ransom demands to stop the attacks or as complex as ancient hostilities that are rooted in religious beliefs.

A cyberwar could be used as a prelude to a real war. The enemy would attack its adversary to cause disruption and confusion prior to a conventional attack. The aim of the cyber-attacks would be to disrupt the communications of the target as well as instill fear and confusion in the populous. This could reduce the will to fight and lead to a quick capitulation. The cyber-attacks would be used like a bombing campaign before an attack. The strategy would be to soften up the enemy before the conventional attacks in a bid for a quick victory (Arquilla & Ronfelt, 1993).

A cyberwar could be fought alongside a conventional war. The attacks would be aimed at vital infrastructures such as water systems, power grids as well as economic entities such as banks, news organizations and ISPs. The cyberwar would be part of the overall struggle between the adversaries. Part of the tactics of any war is to disrupt the enemy's ability to fight the war. Making the economic infrastructure unreliable or unavailable can have the effect of diminishing the fighting capabilities of the enemy (Arquilla & Ronfelt, 1993).

A cyberwar could also be launch at an ally to disrupt or slow down their response to a conventional attack against the intended target. One existing scenario is that if China intended to attack Taiwan, they would first launch an all-out cyber-attack against the United States. The intended effect would be to slow down the American response to the attack on Taiwan and give the Chinese time to establish a foothold in Taiwan. The Chinese would be far more difficult to dislodge once they had established control of Taiwan (Arquilla & Ronfelt, 1993).

A cyberwar could take the form of a cyber cold war. Adversaries would routinely launch attacks at each other and probe each other's systems and defenses. The attacks would be carried out clandestinely so that the target could never be 100% sure who the attacker was. The attacks would gather intelligence on the adversary for use if the war escalated. Since the uncertainty of the Internet allows the attacker to be anonymous this would keep the enemy off balance without the risk of a conventional response (Arquilla & Ronfelt, 1993).

A cyberwar could also be a hot cyberwar. The adversaries would be fully or mostly aware of whom they were fighting but the battle lines would be located only on the Internet. Conventional weapons would not be used at all (Arquilla & Ronfelt, 1993). Disruptions to government, military, civilian, and economic operations could be considerable even without conventional weapons being used. Cyber-attacks would also not require a lull between attacks to allow the forces to regroup. The attacks could be launched at any time, last as long as desired and not require the logistics and supply infrastructure needed for conventional combat.

A cyberwar may not be between governments. Organizations could battle each other, or cyberterrorist organizations could battle countries. For example Islamic jihadis have distributed an electronic program to be used for jihad through their websites. The virtual martyrs with the program would launch attacks against targets that are considered to be anti-Islamic. The distributed program offers a GUI interface that a non-technically skilled individual could use to launch attacks against predetermined targets. The intent of the attacks would be to create economic disruption and to bring down websites. The goal would be to launch attacks on the infrastructure that would cascade through the network and economy, effecting on all members of the intended target (Greenemeier, 2007).

Principles and Operations

Cyberwar has features that make it different from conventional war. The first of these features is that it is relatively cheap to fight a cyberwar. The things needed include personnel who are experts in computer technologies and a computer network with Internet access. It does not require large financial resources or the help of a government to field the planes, ships, tanks or troops needed for a conventional war ("Information Warfare, 1995).

A cyberwar would also have no geographic boundaries. There would be no maps of conquered or lost territory. The boundaries between countries, between military or civilian targets and between private and public segments are blurred in cyberspace. In a cyberwar anything could become a target, no place is safe, and anyone is vulnerable ("Information Warfare", 1995).

Perception can be very easily manipulated in cyberspace. Perception comes from information and information is what is attacked in a cyberwar. Political and social support can be stimulated over the Internet as well as be destroyed. Information about an event can be manipulated and that information can be easily distributed through the Internet. This gives an attacker the ability to control how things are viewed by persons outside of the altercation as well as the people involved. Controlling the messages regarding the struggle allows the controller to garner support for their position and undermine their adversary ("Information Warfare", 1995).

A cyberwar does not have a frontline. A battle could be waged anywhere that has Internet access or a network that can be reached through the Internet. System vulnerabilities may not be well understood, and it could be very difficult to determine who the attacker is and how to best respond to the attack. The Internet was designed to be an open system and allow people access to information. This openness to all users becomes a vulnerability in a cyberwar ("Information Warfare", 1995).

In a cyberwar it would not be possible to know how good an enemy's weapons are until they are used. How good an enemy's hackers are, how vicious their viruses are and how extensive their botnet is would not be known until they are used (Kirk, 2003). An enemy could spend years building up the recourses needed for an all-out attack. These resources include knowledge and expertise. Knowledge about the intended targets could be gathered over time by probing the defenses and by exploring the target systems' footprints. The expertise would be recruited from the best talent that the country or organization had to offer. This pool of talented cyberwarriors would then be trained in the newest and most dangerous technologies. The cyberwarriors could plant logic bombs, Trojan viruses and other malicious code well ahead of any attack (Kirk, 2003).

The Internet does have a physical presence. It exists in conduits under the streets, and in servers and computers that sit in data centers, homes and offices. It exists in ATM machines and POS systems. All of these can be attacked in a cyberwar (Kirk, 2003). The United States has three network nodes that if successfully attacked could shut down communications in the country. A physical attack aimed at just these nodes would be far more devastating than an attack, of similar size, anywhere else (Kirk, 2003). Some targets that experts think would be of interest to attackers would be the power grid, the water systems, 911 systems and the air traffic control systems. Anyone of these would cause major disruption to the economy and to the lives of ordinary people (Kirk, 2003).

Security Threats

Different types of coercion could be used against governments, corporations and individuals in a cyberwar. One of the main intents of any war is to instill fear into the enemy. Fear can be used to coerce an enemy into changing their behavior and it also makes it easier for an adversary to force their will on their foe. The coercion could take the forms of attacks, promises to not attack and demonstrations of destructive abilities against other targets.

Cyber-attacks on corporation systems are considered to be easier to prosecute than attacks on government and military systems. This is due to the limited resources available in corporations and the loopholes created by mergers and acquisitions. The typical hacker that a corporation defends itself against is attempting to gain entry into systems in order to steal information such as identities or credit card numbers. The aim in a cyberwar is to create disruption and economic damage. The motivation is also different. A hacker is motivated by greed and will look for targets that

they feel will offer the biggest reward. If the target is too hardened, they will move on to an easier target. A cyberwarrior is motivated by patriotism and would be willing to spend the time and the recourses needed to crack the intended target (Rasmussen, 2007).

Effects of Cyberwar

An example of the effect that the Internet can have on a conflict is the 1994 Chiapas rebellion in southern Mexico. The Chiapas revolted against the central Mexican government and accused it of neglecting their needs in favor of the wealthy elite in the country. The rebels waged a media and propaganda campaign over the Internet. The rebels spread their story to the world and galvanized public opinion against the Mexican government. The rebels also spread misinformation about the Mexican soldiers stationed in their part of Mexico. The rebels spread information that the soldiers were bombing and strafing the population, torturing and executing civilians, and raping and killing women and children. Most of the accusations were never documented. However, the spreading of the largely false information gave the rebels the upper hand against the Mexican government because of the support that they gained from outside groups and individuals (Knudson, 1998).

Using the Internet the rebels were also able to manipulate and change public opinion. The rebels mixed true and false information to make the Mexican government appear to be the aggressor and were able to spread their views easily and quickly with the use of the Internet. The Mexican government was forced to negotiate with the rebels because they were able to garner news media attention and galvanize public support. This information warfare that was waged against the government of Mexico allowed the rebels to realize at least some of the goals of their rebellion (Knudson, 1998).

This example shows how the Internet can be used to change and control public opinion. Without public support and with outside groups watching every action that the Mexican government took against the Chiapas rebels the government had to proceed very cautiously against the rebels. The rebels were able to change the behavior of the Mexican central government by the use of information warfare and win at least a partial victory. This influence on public opinion is a form of cyberwar that can be used without the need to make direct attacks or create any physical damage.

SCADA Systems

Supervisor Control and Data Acquisition (SCADA) systems are used to control and monitor industrial and infrastructure systems. The systems include gas and oil, air traffic and rail traffic control, power transmission and generation, water supplies and manufacturing. These systems are generally controlled through the Internet because of the ease and cost efficiency that it offers. This also means that the systems could be vulnerable to attack. Electrical blackouts, explosions at refineries, and impure water all could be consequences of cyberwar (Graham & Maynor, 2006).

This vulnerability makes SCADA systems tempting targets in a cyberwar. The systems are of high value to the organization being attacked and provide an avenue of assault through the Internet. The loss of electrical power, water, or refined petroleum products would create serious difficulties for the people affected as well as create economic and environmental damage. It would also have the effect of instilling fear into the population attacked.

Computers seized from members of Al Qaeda showed that the terrorist organization was very interested in SCADA systems. Terrorists operating from outside of the United States could hack into a utility's network and take control of the company's systems. The hackers could then manipulate the control systems and provide false information to the operators. The terrorists could cause damage directly or by providing false information to the operators cause them to perform tasks that would damage the equipment (Kirk, 2003). This scenario shows that terrorist organizations are seriously looking at SCADA systems as possible avenues of attack in a cyberwar.

DISCUSSION

A cyberwar, like a conventional war, would have devastating effects on people and institutions in a country. Society, governments, corporations and individual people would all be affected by the cyber conflict. All of these entities are

necessary for a country to function. If they are not able to function or they are compromised due to a cyberwar the country could falter and become open to outside control or outright defeat. This section will examine the possible effects on each of these entities.

Society

The system that is considered to be the most vulnerable to a cyber-attack is the electrical power grid. Some experts believe that it would be possible to bring a large share of the power grid in the United States down in such a way that it would take six months to fully restore power. This would have a devastating effect on the national economy and on society at large (Kirk, 2003). So much of modern society is dependent on electricity that people would not be able to live or work without it.

A 1977 electrical blackout in New York City was accompanied by massive looting in some locations. Stores were broken into and fires were set. Even more than the toll on property there was a collapse of the social order ("Blackout 2003," 2003). People would expect a blackout to be quickly fixed. If the power grid is damaged in a cyber-attack and takes months to fix the social chaos and unrest will grow. Without power people will not be able to refrigerate food, keep warm in the winter or cool in the summer. Any entertainment systems will not work. Water systems will stop working along with cell phone and Internet communications, as well as fuel delivery systems and banking systems. All of the infrastructures that people rely upon for daily life will grind to a halt. Fear and disillusionment could take over people's lives. As the pressures of everyday survival escalate and people's basic dignity is taken away from them, they will be far more easily threatened and manipulated.

Government

"In theory, the breakdown of one system would compound the effects on another, and the crippling of energy, government services, communications, the media, and health care and finance systems would interact in a downward spiral" (Peters, 2007, para. 6). If an enemy was able to cause that spiral, then military and economic systems could start to fail. Confronted with frightened and panicked citizens a government might be forced to accept surrender or at least a forced armistice.

The pressure on a government to protect its citizens can be intense. As 911 proved citizens are willing to accept and even demand more government control during emergencies. This can change the relationship between the citizenry and the government. The government would be able to do things without question that it would not have under normal circumstances. A cyberwar could force a government to change the way in which it interacts with its citizens and with the rest of the world. A cyberwar's locus is to attack information. It attacks the information that a populous has about itself and its government as well as the information that a government has about its citizens. This information attack causes changes in behaviors that are the intent of the attacker.

Corporations

Most businesses are not prepared for the risk of war, particularly a cyberwar. Just like every member of a society corporations depend upon the basic infrastructure of water and electricity. Without these basic services and with employees concerned about their families and their personal safety it would be difficult for firms to continue to operate in a cyberwar (Rasmussen, 2007). Many experts believe that "large U.S. businesses are in the crosshairs of foreign government entities and terrorists" (Rasmussen, 2007, para. 1). Businesses could be faced with trying to maintain operations during a time when the basic infrastructure is unreliable. The power supply infrastructure could be attacked and unavailable for a period of time. The banking system could also be attacked and cause the ability to process transactions to be lost or interrupted. Transactions such as credit cards, checks, ACH and wire transfer are all processed electronically. Business would not be able to transmit the transactions without electrical power. Companies also would not be able to transmit the transactions if the network between the business and the bank was under attack (Carrubba, 1994).

Any social problems created by a cyberwar would be reflected in business organizations. If the strain of a cyberwar began to cause the loss of the fabric of society, businesses would very quickly see the effects in their employees, customers, suppliers, partners and competitors. The social breakdown could cause employees to not be able to work

because they cannot physically or mentally do their jobs. The business may not be able to pay its employees or suppliers. Its customers may not be able to pay the business. A business may not be able to communicate with its partners and not keep tabs on its competition. The interworking of the economy could falter as systems fail and people lose confidence in the government, society and the future.

Individual

As the cyber-attacks on Estonia showed, people are dependent on information technology for their communications, for their information needs and for their economic transactions. Modern society has built cyberspace so that information can be moved in a cheap, quick and easy manor. This has worked well for individuals and has been embraced by many. People have become dependent on computers and particularly the Internet. To hold government officials accountable for their actions citizens must have access to public records and information. The Internet provides the best way for that information to be disseminated. If that information is not available to individuals then ”elected officials and government bureaucrats could, and some undoubtedly would, hide their mistakes, conceal corrupt practices, disguise favors, and camouflage official actions taken for personal benefit” (Levendosky, 2002, para. 7).

People have become dependent on the Internet and email for news on events taking place. If there was a cyberattack and the news organizations were knocked offline, as happened during the attack on Estonia, people could not be informed. Rumor and speculation would take the place of information. This loss of information and communications would affect people’s relationship with their government and with each other. The isolation that this would create could increase the level of fear that people would feel during a cyberwar and cause them to accept outcomes that they may not have accepted under normal circumstances. The example of the Chiapas rebellion shows that an adversary can control the outcome of a struggle by controlling, or dominating, the information that is available about it. People reply upon information to make decisions and if they have only certain information they will be forced to think in a certain way.

Individuals and their families could also have difficulty with the necessities of life. Their places of employment could be affected so that they are not able to do their jobs. Their employer may not be able to pay them. Their bank may not be able to provide cash or process electronic transactions. Stores may not be able to stock goods to sell or process transactions to sell them. Anything that relies upon electronic information or electronic communications could become unavailable or unreliable. Even the government could be affected and not have the ability to coordinate relief efforts since electronic communication and transactions systems would be unreliable or compromised. Individuals might feel like they are on their own and they may actually be on their own.

A cyberwar, like any war, could have devastating effects on a society, on the government entities and on the businesses and individuals caught up in the war. A cyberwar could, but would not need to, involve physical destruction of property or infrastructure. The effects on information processing and communications transmission would create hardships in of themselves. Information and communications are what hold modern societies together and without them society, governments, businesses and individuals will become isolated and lose hope in the present and the future.

CONCLUSIONS

“There is no such thing as cyberterrorism--no instance of anyone ever having been killed by a terrorist (or anyone else) using a computer” (Green, 2002, para. 6). An expert in cyberwar said that the “United Sates is in the midst of an active cyber-war and is implementing secret security plans for its protection” (Posner, 2007, para. 1). These are two views of the current state of the involvement of the United States in a cyberwar. From the view that cyberwar does not exist to the conviction that the United States is already engaged in one.

In February of 2008 J. Michael McConnell, Director of National Intelligence, reported to the U.S. Senate that, over “the past year, cyber exploitation activity has grown more sophisticated, more targeted, and more serious” (p. 13). McConnell also reports that China and Russia have the capabilities to carry out cyber-attacks against the country. Also, McConnell indicated that terrorist groups have sought the capacity to launch such attacks. The Director also reported that organized criminal elements are continually devising new ways to target and exploit their victims.

The effects of a cyberwar on the United States could be devastating. The effects on individual American, the business economy, the local, state and national governments and society itself could be severe and possibly long lasting. A survey of people, not directly effect by the September 11, 2001 attacks, found that 73 % felt that the attacks had caused them to change the way that they viewed their life (Peters & Thompson, 2003). Cyber-attacks could affect more people and have a wider impact and the effects could last a long time.

The United States does not appear to be currently involved in an open and public cyberwar. The research does indicate that the county could be currently involved in cyber cold wars with both China and Russia. A cold war can be seen as "a condition of rivalry, mistrust, and often open hostility short of violence especially between power groups" ("Cold war," 2008, para. 2).

Both China and Russia are jockeying for more dominate positions in the world. China in particular is trying to assert its position in the world. Some experts believe that China's foreign policy consists of acquiring petroleum and gaining control of Taiwan. Everything else is subservient to those two aims (Friedman, 2005). Both of these goals have the potential to bring China and the United States into conflict. Recent news reports include claims that Chinese nationals working for their government have hacked into computer networks included those of the Pentagon (Vause, 2008). These ongoing hacking activities could perhaps be the information gathering that would take place prior to a larger conflict.

The Moonlight Maze incident, which was attributed to Russia, shows the low-level conflict that is still going on between the two countries. The testing and the probing of defenses could be a prelude to a larger conflict. It could also be a knowledge building activity to provide information for plans in case a larger conflict erupts. Russia's attack on Estonia could also be seen as a test to see the types of effects that cyberattacks could have on a country. The information gathering and the test run against Estonia could possible put Russia into a knowledgeable position in a cyber conflict with the United States.

Both Director McConnell (2008) and the McAfee report (2007) state that organized crime and terrorist organizations are trying to build up the capability to launch cyberattacks. These gorilla organizations would be harder to track and harder to retaliate against in a cyberwar. Since the investment needed to launch a cyberwar would be within the means of some of these types of organizations, they represent another layer of enemies that the United States must guard against.

Technology always offers new opportunities, but it also offers new dangers and requires new ways of thinking about security. Low level cyber conflicts are going on right now that could erupt into all out cyberwar. Governments, the military, businesses, and individuals must be aware of the dangers that cyberwar holds. Societies must gauge those dangers truthfully and make proper plans to respond if it becomes necessary.

More research should be done on the subject of cyberwar. Particular areas that could be examined more closely are the use of information to mold opinions on the conflict such as those done in the Chiapas rebellion. Control of people's opinion could have a powerful effect on the outcome of any conflict cyber or conventional. Also, research could examine how information shapes a society and how an outside force could use its influence in cyberspace to shape how a society sees itself and other societies. Research could examine if subtle influences could be made to cause changes in a society that win a conflict without the affected society ever realizing that there ever was a conflict.

REFERENCES

Aaviksoo, J. (2008). Real threats from the imaginary world. *Vital Speeches of the Day*, 74(2), 28-32.

Abreu, E. (2001). *Epic cyberattack reveals cracks in U.S. defenses*. Retrieved from http://archives.cnn.com/2001/TECH/internet/05/10/3.year.cyberattack.idg/

Anderson, C. (2008). Why $0.00 is the future of business. *Wired*, 16(3), 140-149, 194.

Arquilla, J., & Ronfelt, D. (1993). *Cyberwar and netwar: New modes, old concepts, of conflict*. Retrieved February 23, 2008 from http://www.rand.org/publications/randreview/issues/RRR.fall95.cyber /cyberwar.html

Blackout 2003: The debate we won't be having this time. (2003). Retrieved from http://hnn.us/articles/1633.html

Brenner, S. (2007). At light speed: Attribution and response to cybercrime/terrorism/warfare. *Journal of Criminal Law & Criminology*, 97(2), 379-475.

Carrubba, P. (1994). *Principles of Banking* (5th ed). Washington, DC: American Bankers Association.

Cold war. *Merriam-Webster.com*. Retrieved from http://www.merriam-webster.com/dictionary/ cold%20war

Evron, G. 92007). Estonia cyber-war highlights civilian vulnerabilities. *eWeek*, 24(26), 34-34.

Friedman, T. (2005). *The world is flat*. [Video]. Cambridge, MA: Massachusetts Institute of Technology.

Grant, R. (2008). The dogs of web war. *Journal of the Air Force Association*, 91(1), 22-27.

Greenemeier, L. (2007). *'Electronic jihad' app offers cyberterrorism for the masses*. Retrieved from http://www.informationweek.com/management/showArticle.jhtml?articleID=200001943

Information warfare: A two-edged sword. (1995). Retrieved from http://www.rand.org/publications/randreview/issues/RRR.fall95.cyber/infor_war.html

Jackson, W. (2007). *Greg oslan: The new war machine*. Retrieved from http://www.gcn.com/print/26_25/45086-1.html

Kirk, M. (Writer), & Kirk, M. (Director). (2003). Cyber war! [Television series episode]. In M. Kirk (Producer), *Frontline*. Arlington, VA: Public Broadcasting Company.

Knudson, J. (1998). Rebellion in Chiapas: Insurrection by Internet and public relations. *Media, Culture & Society*, *20*(3), 507-518.

Maynor, D., & Graham, R. (2006). *SCADA security and terrorism: We're not crying wolf*. Retrieved February 29, 2008 from http://www.blackhat.com/presentations/bh-federal-06/BH-Fed-06-Maynor-Graham-up.pdf

McAfee, Inc. (2007). *McAfee virtual criminology report*. Santa Clara, CA: Author.

McConnell, J. (2008). *Annual threat assessment of the intelligence community for the senate armed services committee: 27 February 2008*.

Peters, C., & Thompson, S. (2003). Study on effects of 9011 attacks show most Americans feel more vulnerable. Retrieved from http://www.collegenews.org/x2778.xml

Peters, R. (2007). *Washington ignores cyberattack threats, putting us all in peril*. Retrieved from http://www.wired.com/politics/security/magazine/15-09/ff_estonia_america

Rasmussen, G. (2007). *Cyberwar: A threat to business*. Retrieved from http://searchsecurity.techtarget.com/tip/0,289483,sid14_gci1239371,00.html

Rawnsley, G. (2005). Old wine in new bottles: China-Taiwan computer-based 'information warfare' and propaganda. *International Affairs*, 81(5), 1061-1078.

Robb, J. (2004). *4GW – Fourth generation warfare*. Retrieve from http://globalguerrillas.typepad.com/globalguerrillas/2004/05/4gw_fourth_gene.html

Rowan, D. (2001). The times: Tech column – cyberwar/videophones/osama domains.Retrieved from http://www.davidrowan.com/2001/10/times-tech-column-cyberwarvideophoneso.html

US Senate. http://www.senate.gov/~gov_affairs/030200_adams.htm

Vause, J. (2008). *Chinese hackers: No site is safe*. Retrieve from http://www.cnn.com/2008/TECH/03/07/china.hackers/index.html?iref=newssearch

Webster, W., & de Borchgrave, A (1998). Cybercrime… cyberterrorism… cyberwarfare… Retrieved from http://www.csis.org/media/csis/programs/TNT/cyberfor.pdf.