Cyber Threats and Cyber Security: National Security Issues, Policy and Strategies

Josh White
National and International Security
University of North Carolina at Wilmington
Wilmington, NC 28403
Jrw2633@uncw.edu

Abstract

Cyber security is a growing concern and is increasingly affecting the United States and international community. This research paper identifies the importance of understanding the growth of cyber threats and the cyber security measures the U.S. has enforced. This research paper will also address the cyber security measures the U.S. must adopt in order to reduce and prevent future cyber attacks. This paper examines all scales of cyber threats the U.S. has and may face, by discussing past threats/attacks the U.S. has endured and attacks on an international scale. This paper will include national security measures the U.S. has adopted after these threats/attacks. Cyber threats today pose serious challenges due to rapidly-changing advancements in technology. This paper focuses on providing awareness of cyber threats and cyber security measures that can be adopted as an individual and as a country to prevent future cyber attacks.

Key Words: Cyber Security, Cyber Threats, Modern Technology, Information War, National, Homeland, and International Security

Introduction

Cyber attack is defined by the U.S. Federal Bureau Investigation to be a "premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against non-combatant targets by sub-national groups or clandestine agents" (Rouse, 2010). Cyber threats are acts that are designed to create physical harm or fear or extreme financial harm by accessing certain types of technology and information. Cyber Warfare can include vicious attacks against opponents' computer networks to provide fear/harm, or to paralyze a nation (Lewis, 2002). Cyber threats' primary goal is to access computer network tools in order to shut down critical national infrastructures, such as transportation, energy and government operations (Lewis, 2002). A successful cyber attack could leave a nation's homeland security extremely vulnerable. In today's world, technology continues to advance which leaves many networks and windows of opportunity for cyber attack. Technology advances, as well as cyber threats advances, which forces the U.S. homeland security to constantly develop new preventive security measures. According to author Clay Wilson, cyber threats are greatly on the rise. Reports show that "137,529 computer security incidents were reported to their office in 2003, up from 82,094 in 2002" (Wilson, 2005). The U.S. has endured countless cyber attacks that has gone unknown to the media, as some cyber attacks will not cause physical harm, which can allow these attacks to pass unnoticed due to the normal clutter of everyday life in the U.S.

Cyber Threats and the Media

The media provides hackers with significantly increased opportunities to state their attack or threat to create fear, claim ownership of such actions and secure publicity (Conway, 2006). Cyber attackers can use networks and the internet to bring psychological warfare by posting horrific videos online, delivering threats and recruiting future members. Author *Maura Conway* provides an interesting point, which states "until the advent of the Internet, terrorists' hopes of winning publicity for their causes and activities depended on attracting the attention of television, radio, or the print media" (Conway, 2006). The internet has provided hackers with more opportunity than launching vicious network attacks, but to also project fear by stating their attacks and messages. The internet also allows hackers to have direct control over the content of their messages (Conway, 2006). They may create their own websites to bring awareness of their attacks, to gain attention from the mass media in order to create mass fear among the public. The media is and will remain a problem for national security measures, as homeland security prefers to contain cyber crime within the department. However, due to the mass media, hackers inform the public of their attacks, which creates panic, uncertainty and fear among the public. Therefore the hackers have achieved certain goals and performed a successful attack, even if the damage was not as substantial as they may have planned.

Hackers also tend to use the media as a source of funding. They seek financing both via their Web sites and by using the Internet infrastructure to engage in resource mobilization using illegal means (Conway, 2006). Many will receive their funding or equipment through the internet and will even accept funds via Pay Pal (Conway, 2006).

Media concerns of cyber security use to remain as a non-issue for the U.S. Homeland security, but since the events of 9/11 produced such a large-scale of fear, it has become a focus of the Homeland Security. The events of 9/11 were not only displayed through the homes of the U.S. but through the homes of the entire world. This was the tipping point for the U.S. homeland security. The media is a great advantage for terrorists to gain their goals and it provides plenty of future opportunities in the information war.

Information War

The information war is based on attacks, in which the physical world and virtual world converge. The physical world is the physical matter that is touched, seen and lived every day. The virtual world represents the computer networks and functions that moves the data (Collin, 1997). The intersection of the physical and virtual world, combined with people's dependency on the virtual world creates a great sense of vulnerability to hackers (Collin, 1997). They rely on the vulnerability of the people and of easy-access security networks to allow their attack to be more hostile and effective. Moreover, they are not an average bad actor, since they require a certain skill-set that many will not possess. Their skill-set includes an advanced knowledge of computer networks, data, security networks, information, technology and hacking. Author B. Collin from the journal of *Crime and Justice International* states a brief list of what hackers are capable of; "a hacker could remotely access the processing control systems of a cereal manufacturer to sicken and kill the children of a nation. A hacker could place computerized bombs around a city, all simultaneously transmitting unique numeric patterns, each bomb receiving each other's pattern, so if one bomb stops transmitting, all bombs detonate simultaneously. Moreover, they could disrupt international financial transactions, undermine air traffic control systems, alter the

formulas of medication at pharmaceutical manufacturers, and sabotage utility systems" (Collin, 1997).

Many people suggest or believe a major attack against the U.S. infrastructure is easy, but the truth is it is not. No major attack has happened on U.S. soil since 9/11, despite the countless terrorist groups around the world that make this there primary goal. The U.S. has introduced extensive security measures since the 9/11 attacks, to prevent any similar future horrific acts from occurring. The U.S. has been worried of cyber attacks since the 1990's, so they have been taking extra security measures since then. However, after 9/11 the U.S. increases cyber security measures in fear of a cyber attack against the U.S. infrastructures (Janczewski & Colarik, 2008).

Authors Lech Janczewski and Andrew Colarik of *Cyber Warfare and Cyber Terrorism* provide three reasons of why a hacker of the information war will commit a cyber attack. The first reason is the fear factor. The fear factor is "the most common denominator of the majority of attacks is a terrorist wishes the creation of fear in individuals, groups, or societies. Perhaps the best example of this drive was the bombing of a Bali nightclub in 2002. This nightclub was nothing other than a watering hole for foreign tourists (Australians in particular), and inflicting casualties and fear among them was the main objective of the attackers. The influx of foreign tourists to Bali was significantly reduced after this attack. The same applies to attacks against IT installations" (Janczewski & Colarik, 2008). The second reason is the spectacular factor. The spectacular factor is the idea that the cyber attack should have a spectacular nature. The spectacular attack consists of an attack aimed at creating huge direct losses and in resulting to lots of negative publicity. The third reason is the vulnerability factor, which states that cyber activities will not always result to huge financial losses. Many cyber attacks focus on demonstrating an organization's vulnerability by causing a denial of service to the commercial server or defacing an organizations webpages, which is also known as computer graffiti (Janczewski & Colarik, 2008).

Today many cyber attacks specifically target finances, which can also then be used to support other terrorist attacks. The FBI/CSI 2006 Computer Crime and Security Survey states that virus attacks continue to be the main source of the greatest financial losses. The second-greatest source of financial loss is unauthorized access (Janczewski & Colarik, 2008).

An important vulnerability that must be secured from cyber attacks are the DNS and Routing system. Domain Name System (DNS) is the tool that recognizes internet addresses. If a hacker could hack into a DNS, they would be able obtain information by forwarding all types of information to themselves. The defense technology in preventing attacks against DNS is secure. However, a well-designed attack could create havoc in the network world and release unauthorized information that could be acted upon by a future attack (Janczewski & Colarik, 2008). In the past there have been many cyber attacks that resulted to the release of unauthorized information, which then progressed into another form of an attack.

Past Cyber Threats and Attacks

In July 1997, the leader of a Chinese hacker group claimed responsibility of a cyber attack that had temporarily disabled a Chinese satellite and stated that he was forming a new global hacker organization to protest and disrupt Western investments in China (Janczewski & Colarik, 2008).

In 1998, a terrorist guerrilla organization executed a cyber attack that flooded Sri Lankan embassies with 800 e-mails a day for a two-week period. The e-mails simply stated, "We are the

internet Black Tigers and we're doing this to interrupt your communications." Security intelligence departments categorized it as the first known attack by terrorists against a country's computer systems (Janczewski & Colarik, 2008).

In September 1998, on the evening of Sweden's general election, hackers defaced the Web site of Sweden's Right-wing political party and created links that directed to the home pages of the left-wing party and pornography sites (Janczewski & Colarik, 2008). Also in 1998, cyber-terrorists rewrote the home page of a Mexican government Internet website to protest what they said were instances of government corruption and censorship (Janczewski & Colarik, 2008).

In 1999, the Amazon Web site was attacked and shut down for some time due to a denial of service (DOS) attack. The Amazon website suffered many losses due to suspended trading and the attack received widespread publicity throughout the world (Janczewski & Colarik, 2008).

In 2000, a former, disgruntled employee hacked into Maroochy Shire, which is an Australian waste management control system and released millions of gallons of raw sewage into the town. (Janczewski & Colarik, 2008).

In 2001 the U.S. suffered from the biggest terrorist attack recorded; 9/11. The 9/11 attacks also resulted to the greatest cyber attack in the U.S. The 9/11 attacks against the World Trade Center and the Pentagon, which destroyed computer databases and disrupted military and civilian finances and communication systems. The loss of communication effected the financial markets, as all markets closed up to a week (Wilson, 2005).

Many successful cyber attacks do follow up with a physical attack, such as the Operation Desert Storm in 1991. The U.S. military disrupted Iraqi communications and computer systems by launching cruise missiles to scatter carbon filaments that short circuited power supply lines (Wilson, 2005).

The U.S. Homeland Security has always taken extra security measures to prevent any cyber attack from occurring. However, it is impossible to prevent all forms of cyber attacks. According to NATO's website, in December 2006 NASA blocked all emails with attachments before the shuttle launched, as they were worried it would allow hacking into their network. The following week there was an announcement that unknown hackers had obtained the recent plans of the U.S. space ship vehicles (NATO, 2013).

In June 2007, the U.S. Secretary of Defense's email was hacked into by an unknown attacker. The hacker focused on accessing and exploiting the Pentagon's networks. In 2008 the databases of both the Republicans and Democrats campaigns were accessed by an unknown foreign cyber-terrorist (NATO, 2013).

In January 2009 Israel's internet infrastructure underwent a cyber attack which was correlated with Israel's offensive in the Gaza Strip. The cyber attack focused on Israel's government websites and was executed by an estimate of five-million computers. The cyber-attack was believed to have been executed by a criminal organization based in a soviet state, and paid for by Hezbollah or Hamas (NATO, 2013).

In January 2010 a hacker organization called the 'Iranian Cyber Army' attacked a popular Chinese search engine, called Baidu. Users of the search engine were directed to a webpage that showed a certain Iranian political message. Several months earlier, the 'Iranian Cyber Army' also executed a cyber attack on twitter, which displaced a similar Iranian message to Baidu (NATO, 2013). In October 2010, stuxnet was found in Iran and Indonesia, that was believed to be a government cyber weapon aimed at the Iranian nuclear program. Stuxnet is a complex tool that is designed to interfere with Siemens industrial control systems (NATO, 2013).

In 2011 the Canadian government reported a huge cyber attack against their agencies, such as the Defense Research and Development Canada, which is a research agency for Canada's Department of National Defense. The cyber attack forced the Treasury bond and finance department, which are Canada's main economic agencies, to disconnect from the internet (NATO, 2013).

In October 2012, the world experienced a large-scale, cyber attack. The cyber attack was called 'Red October' and it was reported to have been operating for five years. The hackers gained information through Microsoft's Word and Excel programs (NATO, 2013). The cyber-attack targeted countries in Eastern Europe, former USSR, central Asia, Western Europe and Northern Europe (NATO, 2013). The attack gained information of all countries government embassies, military instillations, energy providers, research firms, nuclear and other critical infrastructures (NATO, 2013). In 2013 NATO released a statement in regards of their advancements in cyber security, in order to protect NATO and their alliances. "The NATO Computer Incident Response Capability (NCIRC) upgrade project, a 58 Million euro enhancement of NATO cyber defenses, is on track for completion by the end of October 2013. This major capability milestone will help NATO to better protect its networks from the increasing number of cyber attacks against the Alliance's information systems" (NATO, 2013).

The most recent well-publicized, cyber attack against a U.S. company was the attack against Sony in regards to releasing the movie, 'The Interview'. The FBI reported that North Korea was responsible for the cyber attack that hacked into Sony's emails and released embarrassing emails and personal details about star actors. The hacker-group also released a statement that a 9/11-type attack will be executed if the cinemas play the movie. The premiere of the movie was canceled. However, Sony ends up showing a limited release of 'The Interview', as the U.S. did not want to give in to any terrorist requests. Several days later, the U.S. imposes sanctions on North Korea in response to the cyber attack. Also North Korea suffered a severe internet outage in response to the cyber attack against Sony.

Homeland Security

The Department of Homeland Security has an important mission to ensure the homeland is safe, secure and resilient against terrorism and other hazards (Security, 2015). The Website of the *Department of Homeland Security* states that the "hundreds of thousands of people from across the federal government, state, local, tribal, and territorial governments, the private sector, and other nongovernmental organizations are responsible for executing these missions. These are the people who regularly interact with the public, who are responsible for public safety and security, who own and operate our nation's critical infrastructures and services, who perform research and develop technology, and who keep watch, prepare for, and respond to emerging threats and disasters. These homeland security professionals must have a clear sense of what it takes to achieve the overarching vision articulated above" (Security, 2015). After 9/11 the department of homeland security took serious measures in improving their networks and enforcing stricter security in all aspects of the nation, and in specifically cyber attacks. The department has the leading role for protecting all civilian government computer systems and works with tribal, local, state, industry and territorial governments in order to secure critical and information systems (Security, 2015).

The department focuses on analyzing and reducing cyber threats and vulnerabilities. Homeland security also focuses on distributing threat warnings, coordinating responses to the

cyber incidents to ensure that our networks, infrastructures, computers, and cyber systems remain safe (Security, 2015). The department of homeland security has increased its employees and resources in the Cyber Crime Center and are becoming more involved in different cyber-crimes. The new list of cyber crimes that are being perpetrated through cyberspace are child exploitation conspiracies, production and distribution of child pornography, intellectual property violations, banking and financial fraud, and other crimes which have substantial economic and human consequences (DHS, 2015). The DHS states that the Cyber Crimes Center focuses on offering "cyber crime support and training to federal, state, local, and international law enforcement agencies. C3 also operates a fully equipped computer forensics laboratory, which specializes in digital evidence recovery, and offers training in computer investigative and forensic skills" (DHS, 2015). The *DHS* describes the potential threat the U.S. may face and must secure itself from, is the "growing concern that is the cyber threat to critical infrastructure, which is increasingly subject to sophisticated cyber intrusions that pose new risks. As information technology becomes increasingly integrated with physical infrastructure operations, there is increased risk for wide scale or high-consequence events that could cause harm or disrupt services upon which our economy and the daily lives of millions of Americans depend" (DHS, 2015).

The Department of Homeland Security focuses on securing cyber space by utilizing the cyber security and law enforcement capabilities to safeguard and prevent any cyber crimes. Law enforcement agencies play a major role in providing the nation's security by investigating a wide range of cyber crimes, from theft and fraud to child exploitation, and they apprehend and prosecute those who are guilty (DHS, 2015). Law enforcement agencies are also responsible for reporting any cyber attacks they discover to state, local, territorial and federal agencies.

The DHS also works with other components such as U.S. Immigration and Customs Enforcement (ICE) and the U.S. Secret Service. The ICE works with homeland security in supporting domestic and international investigations into cross-border crimes. The U.S. Secret Service uses an electronic task force, which focuses on locating and identifying cyber criminals linked to cyber intrusions, data breaches, bank fraud and other computer-related crimes (DHS, 2015). The Secret Service Cyber Intelligence has directly prevented many cyber attacks and has arrested countless cyber criminals that are responsible for theft and fraud of millions of credit cards, which has approximately resulted to the loss of over six-hundred million dollars. The Secret Service is also responsible for running the National Computer Forensic Institute, which provides law enforcement, judges and prosecutors a variety of cyber training and information to combat cyber-crime (DHS, 2015).

The Department of Homeland Security contains many departments within that are assigned certain duties in order to maintain a cyber secure nation. The National Cybersecurity Protection System (NCPS) provides threat detection, advanced analytics, information sharing and threat prevention capabilities to prevent and combat cyber threats to the Federal Executive Branch networks and information (DHS, 2015). The capabilities of the NCPS provide "a technological foundation that enables DHS to secure and defend the federal civilian government's information technology infrastructure against advanced cyber threats" (DHS, 2015). One of the main DHS key technologies within NCPS is to provide an early threat detection warning of any form of cyber threat to the federal government, provide a detailed identification of the potential cyber attack and state the intended prevention of the cyber attack. Another department that was formed within the Department of Homeland Security is the Continuous Diagnostics and Mitigation (CDM) program that was established by Congress. The

program is responsible for providing adequate, cost-effective, risk-based cyber security and efficiently distribute cybersecurity resources (DHS, 2015). The DHS also has a National Cybersecurity and Communications Integration Center (NCCIC) that is a 24/7 situational awareness and threat management center. The NCCIC's Computer Emergency Readiness Team (CERT) provides advanced network and digital media analysis expertise to identify cyber-attacks focused on attacking the United States networks. CERT has a major role in distributing important information regarding possible cyber threats to all federal and local agencies. CERT works to reduce the risk within all infrastructure sectors. "Cyber security and infrastructure protection experts from ICS-CERT provide assistance to owners and operators of critical systems by responding to incidents and restoring services, and analyzing potentially broader cyber or physical impacts to critical infrastructure" (DHS, 2015). CERT is also responsible for operating NCPS to locate cyber threats and determine what the best prevention is.

In order to improve critical infrastructure cybersecurity, the DHS established a program called Critical Infrastructure Cyber Community Voluntary Program to specifically focus on the U.S. infrastructures and the cyber risk management processes. The program "aims to support industry in increasing its cyber resilience; increase awareness and use of the Framework for Improving Critical Infrastructure Cybersecurity; and encourage organizations to manage cybersecurity as part of an all hazards approach to enterprise risk management" (DHS, 2015). The DHS also established the National Infrastructure Coordinating Center (NICC) to maintain alertness of the U.S. critical infrastructure for the federal government. When an incident does occur the NICC helps share and explain information between the owners/operators and the Department of Homeland Security, and helps secure all vital assets (DHS, 2015). "The NICC and the NCCIC share cyber and physical security information to enhance the efficiency and effectiveness of the U.S. government's work to secure critical infrastructure and make it more resilient" (DHS, 2015).

Potential Cyber Attacks

The main sources of potential cyber attacks stem from terrorist groups, targeted nation-states, terrorist sympathizers and anti-U.S. hackers, and thrill seekers. A prime example of terrorist sympathizers are the individuals that sympathize for both sides of the Kashmir conflict between Pakistan and India. The individuals used cyber tactics to disrupt each other's information systems and disseminate propaganda. As a result pro-Pakistan hackers of the conflict hit Indian sites extra hard (Vatis, 2001). After the 9/11 attacks, there has been a dramatic increase in numbers of terrorist sympathizers and anti-U.S. hackers, and these numbers continue to grow. There is a real danger of any group that resents the U.S. and its allies could potentially create a large and diverse coalition of cyber-attackers. Also there is a danger that Chinese hackers may become involved with the coalition of cyber attackers, as they may still feel resentment towards the U.S. and believe they have scores to settle. Chinese hackers may still feel uneasy about the American surveillance plane colliding with their fighter plane and they remain angry about the NATO accidental bombing of the Chinese embassy in Belgrade in 2000 (Vatis, 2001).

For thrill seekers, any form of conflict that "plays out in cyberspace will invariably attract a huge number of hackers and script kiddies who simply want to gain notoriety through high profile attacks" (Vatis, 2001). Thrill seekers are not usually politically or ideologically driven, but they tend to share the desire to achieve acknowledgment for succeeding in a cyber attack.

Normally the level of skill and sophistication of the cyber attacks are low and the threat to the U.S. systems are low. However, the likelihood of attacks from thrill seekers is extremely high due to the large media coverage that follows these certain attacks (Vatis, 2001). An example of a thrill seekers attack are the DDoS attacks against websites, such as CNN and Yahoo in February 2000. Also the attack included various computer worms and viruses that caused major disruptions among computer systems (Vatis, 2001).

An example of targeted nation-states are the cyber attacks that were directed against North Atlantic Treaty Organization (NATO) infrastructures as allied air strikes hit Former Republic of Yugoslavia (FRY) targets in Kosovo and Serbia. NATO webservers experienced attacks by hackers from the FRY military. One-hundred of NATO's webservers experienced DDoS assaults and thousands of e-mails that contained damaging viruses. As a result of the attack, NATO servers were brought to a halt for a number of days (Vatis, 2001). The author *Vatis* states that "many foreign nations have identified the utility of developing cyber attack techniques for purposes of engaging in covert espionage against U.S. government networks or U.S. industry, or for employing information warfare against the U.S." (Vatis, 2001). It is expected that the U.S. will be a target of information warfare by China, North Korea, Cuba, Russia, Iraq and Libya. An extreme possibility the U.S. is anxious of, is if a nation launches cyber warfare against the U.S., there is a possibility that the nation could disguise the origins of the attack, and make it appear to look like a cyber attack from one of U.S.'s allies (Vatis, 2001).

Hacker groups are not well-known to use cyber attacks as their primary source of attack, but terrorist groups are constantly using technology and the Internet to develop plans, raise funds, communicate securely and spread propaganda. However, as a result of the financial information infrastructure in New York City being destroyed due to the 9/11 attacks, terrorist groups are attempting to advance in using more and more cyber-attacks as time elapses to focus on destroying other U.S. infrastructures. The U.S. has to be more careful of modern terrorist cyber-attacks that will attempt to destroy U.S. infrastructures, which will be followed by a physical terrorist attack.

Cyber attacks may also stem from political tensions between nations. An example of a political tension cyber attack is when a U.S. surveillance plane collided with a Chinese fighter plane on April 1st, 2001. The political tension between the two nations was enforced by an online campaign of mutual cyber attacks. The cyber attacks included website defacements, which both nations were capable of due to an immense support of hackers. Approximately one-thousand and two-hundred U.S. websites were subjected to DDoS attacks or were defaced with pro-Chinese images. Such American websites included those belonging to the White House and other government agencies (Vatis, 2001).

There are potential attacks the U.S. may always be at risk from, such as Web Defacements and Semantic Attacks, Domain Name Service Attacks (DNS), Distributed Denial of Service Attacks (DDoS), Worms, Routing Vulnerabilities, Infrastructure Attacks and Compound Attacks (Vatis, 2001). Web Defacements and Semantic Attacks will normally remain politically motivated and the most hostile web defacement would involve a semantic attack. Semantic attacks will usually target news sites, government agency sites or military sites and will cause the websites servers to provide false information (Vatis, 2001). Domain Name Service Attacks (DNS) change the numerical address of the website, which would force the user to an incorrect server, while the user believes he is on the correct server. The likelihood of a DNS attack will only increase during the war on terrorism. Distributed Denial of Service Attacks (DDoS) are normally against high value targets, which will dramatically increase during the war

on terrorism and to defend against these attacks remains a great task. The main targets for DDoS attacks are chat and mail servers, high volume sites, government websites, and news services (Vatis, 2001). Worms are able to go un-detected and cause major problems in the information infrastructure. Recent analysis of ISTS scientists states that worms are capable of doing much more damage with minor alterations. It is believed that "Hybrid worms that combine a series of historically successful exploits to maximize effectiveness are certain to appear in the near future, if not during the war on terrorism. Inevitably, there will be new worms based on vulnerabilities that are not yet known, and therefore, not immediately patchable" (Vatis, 2001). Routing Vulnerabilities have a lack of diversity in router operating systems, which could allow for a major routing attack. A potential target for a routing attack is the border gateway protocol (BGP), which its routers use to make decisions on where to send traffic on the Internet. The result of the routing attack would leave a 'black hole' where large amounts of information headed for destinations all over the world would lost (Vatis, 2001). Infrastructure attacks will always remain a potential attack of terrorists, as it attacks the core of a nation and has the potential to bring a nations homeland security to its knees. Potential infrastructure attacks will mainly target a nation's banking and financial, voice communication systems, electrical infrastructures, oil and gas, and water resources (Vatis, 2001). Compound attacks include a multi-faceted attack retaining some or all of the attack scenarios. The author *Vatis* states that "a compound cyber-attack by terrorists or nation-states could have disastrous effects on infrastructure systems, potentially resulting in human casualties. Such an attack could also be coordinated to coincide with physical terrorist attacks, in order to maximize the impact of both" (Vatis, 2001).

Preventive Recommendation Measures

In order to prevent any cyber attack the nation must be on high cyber alert during the war on terrorism. All departments within the Department of Homeland Security must remain on high-alert at all times and constantly searching to detect any potential cyber threats. System administrators and government officials within the U.S. and allied countries must also stay on high alert for any warning signs of hostile cyber activity (Vatis, 2001). Additional precautions must be in effect in order to sustain a cybersecurity. Such additional precautions may include logging levels to be temporarily raised to trap as many cyber threats as possible. Another additional precaution would be to assign the NIPC and other appropriate entities to issue specific warnings to potential victims (Vatis, 2001). "Systematic and routine risk assessments of information infrastructures provide a good starting point for effective risk management and thus should be a priority" (Vatis, 2001).

To prevent cyber attacks in the future the U.S. must maintain a system that follows an organization's standard operating procedures. The standard operating procedures should ensure operating systems and software be updated regularly, strong password policies should be enforced, systems should be 'locked down', all unnecessary should be disabled, high fidelity intrusion detection systems and firewalls should be employed, and antivirus software should be installed and kept up to date (Vatis, 2001). All security measures that are believed to be excessive, must now be seen as minimal efforts of security.

To prevent any cyber attacks it is important that a nation must secure critical information assets. All services that have the potential to suffer serious communications failure or financial loss from a cyber attack should be considered a critical information benefit. As it is too costly to

protect all systems, measures should be taken to protect and secure all critical systems. "Anti-defacement measures include checks for characters associated with popular web server exploits. Border routers should make use of existing authentication mechanisms to prevent malicious tampering with routing tables. Domain name servers should be running only recent and secure software to prevent DNS corruption and the redirecting of web traffic to bogus sites" (Vatis, 2001). In case of a cyber or physical attack, all important data should be regularly backed up and kept off-site to prevent any loss of data. To prevent any internal cyber attacks within a department, all log records should be carefully monitored, copied and stored in a secure location.

Also to prevent any cyber attacks in the U.S., it is important to enforce ingress and egress filtering. Spoofed IP addresses are normally easy to detect and can be easily discarded of. The egress filtering discards the outbound IP address, which is fairly simple but not widely used as a procedure. Ingress filtering can locate any un-trusted source IP address and discard of the source before it enters the network, which can also be very effective. Untrusted source addresses are normally private networks or networks that have not yet been issued by the international authorities that assign Internet numbers (Vatis, 2001). The author *Vatis* discusses important cyber preventive measured for the DDoS to "include cooperation from upstream Internet service providers (ISPs) that send packets to their client networks. ISP routers can be programmed to limit the rate at which packets typically associated with attacks (SYN and ICMP packets) are sent downstream to client networks. By rate limiting these particular packets, the effects of a malicious flood can be minimized without seriously disrupting normal operations. These preventive measures are well within the capabilities of most Internet service providers." (Vatis, 2001).

Another potential recommendation for preventing a cyber attack is to develop a successful and well-detailed IP trace-back scheme, which can locate the actual source of attack of a Denial of Service attack (DoS) and DDoS attack. A successful trace-back scheme would have the potential of identifying the actual attacker. In order for a successful trace-back scheme to work, it must include automatic trace-back to speed up tracing and reduce human intervention (Gao & Ansari, 2005). It must also include capabilities to identify the indirect source of reflector-based DDoS attacks and capabilities to identify the attacker who conceals themselves with stepping stones. The trace-back scheme should also integrate IDS or defensive measures with trace-back, to allow one mechanism to perform tracing, detection and defense (Gao & Ansari, 2005)

References

Collin, B. (1997). Future of Cyberterrorism: The Physical and Virtual Worlds Converge. *Crime and Justice International*, 15-18.

Conway, M. (2006). *Terrorism and the Internet: New Media-New Threat?* Dublin: Parliamentry Affairs.

DHS. (2015, September 22). *Department of Homeland Security*. From Cyber Security Overview: http://www.dhs.gov/cybersecurity-overview

Gao, Z., & Ansari, N. (2005, May). Tracing Cyber Attacks from the Practical Perspective. *IEEE Communications Magazine*, 123-131.

Janczewski, L. J., & Colarik, A. M. (2008). *Cyber Warfare and Cyber Terrorism.* New York: IGI Global.

Lewis, J. A. (2002, December). Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats. *Center for Strategic and International Studies*, 1-12.

NATO. (2013). *NATO Review*. From The History of Cyber Attacks: http://www.nato.int/docu/review/2013/cyber/timeline/EN/index.htm

Rouse, M. (2010, May). Tech Target. *Cyberterrorism Definition*.

Security, H. (2015, July 16). *Homeland Security*. From http://www.dhs.gov/our-mission

Vatis, M. A. (2001). *Cyber Attacks During The War On Terrorism: A predictive Analysis.* Hanover: Institute For Security Technology Studies At Dartmouth College.

Wilson, C. (2005). Computer Attack and Cyberterrorism: Vulnerabilities and Policy Issues for Congress. *CRS Report for Congress*, 1-46.