Cyber-Security: The Threat of the Internet

Brianna Heidenreich
Political Science and Economics
University of North Carolina
Chapel Hill, NC 27514
heidenre@live.unc.edu

David H. Gray
Campbell University
Buies Creek, NC 27506
grayd@campbell.edu

Abstract

The security of Americaôs infrastructure has been identified as one of the Nationôs most urgent and complex challenges. This paper addresses the growing importance of cybercrime and cyber-security within the United States as advancements of the Internet have led to these non-traditional security concerns. This paper examines this national security issue through analyzing terrorist media tactics, network vulnerabilities and threats, Americaôs interconnected infrastructures, international partnerships, and the solutions, regulations, and policies towards protection. Todayôs information age presents society with unlimited possibilities for our future, as well as threats against it. This paper aims to raise awareness of these issues and the choices we have as users within cyberspace.

Key Words: Cybercrime, Cyber-security, Terrorism, Homeland Security, Department of Defense, Media Messages, TRUST, United States, National Security, Counterterrorism

Introduction

The creation of the Internet has always held unlimited possibilities. However, its emerging technology and ideal have been challenged by pornographic and racist content, as well as developed into one of the number one sources of International Terrorism. Today, radical terrorists of various kinds ï anarchists, nationalists, separatists, revolutionaries, neo-Marxists, and fascists ï are using the network to distribute their propaganda, to communicate with supporters, to create followers, and to overall execute their operations (Weimann, 2005). It has become sadly ironic that the internet began with a network system created by the U.S. Department of Defense (ARPA) with motivations to subside fear of a nuclear attack from the Soviets, as now (although much better developed) this same network serves as one of the largest threats against the United Statesô security services (New Media Institute, 2012). The first known fully operational packet-switching network (predecessor to the internet), ARPA, was designed to facilitate communication between the Defense Departmentôs ARPA computer terminals during the early 1960s, at a time when computers were far too expensive for widespread usage. The primary motivating factor was to efficiently link multiple computers together allowing access to data without the waste of time and travel, which would also aide the U.S. Military in developing a survivable communication structure in the event of a nuclear attack (New Media Institute, 2012). Today, we are witnessing a network with capabilities to attack the very society we had planned to protect.

Modern Terrorism through Society's Media

The Internet, now as powerful as ever in the present day, with international connections and a decentralized structure serves as the ideal network for terrorist capabilities. Due to this access of terror through ñmedia,ò communication scholars now conceptualize modern terrorism within the framework of symbolic communication theory, as Philip Karber, author of *Urban Terrorism: Baseline Data and Conceptual Framework,* states, ñas a symbolic act, terrorism can be analyzed much like other media of communication, consisting of four basic components: transmitter (the terrorist), intended recipient (target), message (bombing, ambush) and feedback (reaction of target audience (Weimann, 2005).ò There have also been arguments made claiming that terrorism is theater, aimed not at the actual victims, but at the audience watching these victims through their television screens. Modern Terrorism can then be understood as an attempt to communicate messages through the use of orchestrated violence. ñMessages of Violenceò are illustrated easily as the news media is able to carry the scenes of death and destruction from terrorism into our homes, and then transfer these same scenes of fear to the homes of terrorists (Weimann, 2005).

Cybercrime: Modern Terrorism

Modern Terrorism has increasingly grown in importance through ñmediaò, specifically following the events of 9/11 (Franceschetti, 2011). This growth has created the need for cyber-security within the divisions of Homeland security of the United States. These new media concerns of cyber-security protection were once categorized as ñnon-traditional/non-conventional issuesò as the past has only focused on ñtraditionalò issues of security threats (Kshetri, 2013).

Examining various terrorist attacks from the past will illustrate the urgency and need for cyber-security and Homeland security efforts at all times. In 1995, the Tokyo Chemical sarin attack occurred, where terrorist developed their own capability to produce sarin through investing in scientists and skilled workers with a facility in Japan. This attack caused 12 deaths and contaminated nearly 5,500 people after the terrorists had released sarin liquid into subway cars. In 2005, the Murrach Building attack occurred in Oklahoma City, killing 167 people and injuring 853 people. This occurred through the creation of a bomb by terrorists, with materials found in department stores. In 2009, the US electric grid was penetrated by an unknown source. This grid covers three separate electric networks, covering the East, West, and Texas. These utilities are operated under Internet-based communication, causing it to be extremely vulnerable to hackers and spies. The intruder was never identified. Attacks such as these are after infrastructures, people, symbols, and information ï all driven by different motivations, making it extremely difficult to design specific countermeasures to address all of them (Franceschetti, 2011).

Following September 11, 2001, the World Trade Center Bombing, Homeland Security activity greatly increased, with wider perspectives and developments towards improving our counterterrorism measures (Franceschetti, 2011). Their sole mission became focused on the development of procedures and techniques for an early warning of threat, and effective countermeasures. Through these developments it has been realized that cyber-security measures and measures against all non-conventional terrorism are extremely imperative for our nationôs safety. The terrorist attacks mentioned above illustrate the non-conventional methods of terror that Homeland Security aims to prepare for. To better understand these non-conventional terrorist methods, it is best to define them. Most security professionals would define non-conventional terrorism as any use by terrorist elements of Weapons of Mass Destruction (WMDôs) which include chemical agents, that can cause death, illness, or injury, and nuclear weapons. Today, with the growing importance of Internet communication and cyber-security technologies, ñWeapons of Mass Disruptionò which can disrupt or destroy electronic equipment, are also considered in this

non-conventional terrorism category. Overall, these non-conventional methods can be categorized under the definition of terrorizing ñindirectly,ò making it even more difficult for responders to respond and attack the instigators (Sharhar, 2005).

In 2009, drunken vandals in Morgan Hill, California cut phone and Internet cables ï causing a serious problem for the nearby area. Santa Clara, San Benito, and Santa Cruz completely lost services in credit cards, ATMôs, ambulances (emergency requests), and basically all modern conveniences which rely on power. This event disrupted life for the people living in the area for an entire day. This event illustrates how easily our lives can stop and the thought of the possibility of similar events in the future is extremely disturbing (Franceschetti, 2011). Without proper cyber security protection, the society we have constructed is in danger and is extremely unstable. All the systems that our society is composed of are made up of interconnected systems and the failure of one will affect the rest. In order to maintain our lives of safety and productivity we must protect the critical systems upon which our economy and society depend on (Franceschetti, 2011).

Terrorism Networks

Unfortunately, the set-up of the Internet is extremely terrorist friendly. It is decentralized and therefore without controlling subject or restriction, it is not censored, and anyone can use it (Weimann, 2005). The anonymity of the Internet is also very attractive to terrorists as their extremist beliefs and values require anonymity in order to exist and operate in social environments that do not agree with their ideology or activities. The structure of modern terrorists also favor the loosely knit network of cells, divisions, and subgroups found on the internet ï typical to the structure system of modern terrorists, who can now maintain communication via internet networks. This terrorist network is referred to as ñNetWar,ò where conflict and crime are now being organized through small groups who communicate and coordinate through ñinternettedò manner and without a specific central command. According to former CIA counterterrorism Chief Vince Cannistraro, ñInternet communications have become the main communications system among al Qaeda around the world because itôs safer, easier and more anonymous if they take the right precautions, and I think theyôre doing that (Weimann, 2005).ò

Al Qaeda actually had a long-lasting website, alneda.com, where al Qaeda members created a fictitious organization, ñThe Center for Islamic Studies and Research,ò and then wired $87 dollars to a Malaysian bank to pay for the cost of the website for a year. Terrorists also rely on using e-mail, chat rooms, e-groups, forums, and virtual message boards, allowing for effective communication bases for operation (Weimann, 2005). Terrorist groups can then connect with members of other terrorist groups, where they can exchange ideas and information on how to build bombs, establish terror cells, and carry out planned attacks. A research project hosted by the United States Institute of Peace summarized seven years of terrorist presence on the Internet and found that all active terrorist organizations maintain websites (Weimann, 2005). This research project also found that terrorists were found to use the internet as we all do ï through gathering and communicating, or by gathering funds for propaganda much like political organizations. However, they were also found to behave in more unusual ways such as hiding instructions, manuals, and directions in coded messages or encrypted files. Itôs interesting to note how al Qaeda operatives used the internet to defend the attacks of 9/11, as they stated on their two websites ï alneda.com and drasat.com that, ñIslam shares no fundamental value with the West and that Muslims are committed to spread Islam by the sword (Weimann, 2005).ò The Internet is also used by terrorists to deliver threats and messages to enemy governments as well as harm the credibility of enemy media and officials (Weimann, 2005).

This effective and direct communication by terrorists creates a huge advantage for terrorism networks, however the information the Internet provides them is also critical to their efforts. The

Internet provides terrorists with information regarding the schedules and locations of targets such as transportation facilities, nuclear power plants, public buildings, airports and ports, or even todayôs counterterrorism measures against their very actions. Terrorists also have access to maps, images, photographs, directions, codes, and exact details of how to use explosives. Searches of online newspapers and journals allow a terrorist to study the strategies designed to stop his actions, or the vulnerabilities to these options. Dan Verton, the author of *Black Ice, The Invisible Threat of Cyber-Terrorism*, explains that, ñal Qaeda cells now operate with the assistance of large databases containing details of potential targets in the U.S. They use the internet to collect intelligence on those targets, especially critical economic nodes, and modern software enables them to study structural weaknesses in facilities as well as predict the cascading failure effect of attacking certain systems (Weimann, 2005)ò.

Online searching capabilities on the internet allow terrorists to capture data with anonymity and without expense. For example, a once captured al Qaeda computer contained information regarding the engineering and structural features of a dam ï allowing al Qaeda engineers the information to design catastrophic failures of that dam. According to Secretary of Defense Donald Rumsfeld, an al Qaeda training manual recovered in Afghanistan states, ñUsing public sources openly and without resorting to illegal means, it is possible to gather at least 80% of all information required about the enemy,ò can you imagine the absolute tragedies that can or have been simulated due to the information that the Internet provides to just anyone (Weimann, 2005)? *The 9/11 Commission Report,* also noted that ñTerrorists could simply buy off the shelf and harvest products of a $3 trillion a year telecommunications industry.ò They could acquire without great expense communication devices that were varied, global, instantaneous, complex, and encrypted (Weimann, 2005). It is recommended that, ñas citizens spoiled with the eases, technology should become more aware of the dangers it also holds as is even assumed that the advancements within todayôs technologies enable terrorists to operate with a decreased need for government protection as technologies such as encryption allow a terrorist group to operate with quite the safety net (Baer et al, 2005).ò On the Internet one can even find two well-known terrorist bomb manuals ï the *Terrorist's Handbook* and *The Anarchist Cookbook (*Weimann, 2005*).* The Hamas organization actually has an Internet course that offers 14 lessons in bomb making with tests administered after each lesson. Al Qaeda also uses the Internet as a virtual training camp. When American forces shut down al Qaeda training camps, they simply moved their operations to the Internet, and experts now refer to this as an ñonline terrorism universityò (Weimann, 2005). This move increases the ñtrueò terror of terrorism through the added aspect of pure chaos that the Internet provides. The availability of terror online allows for further decentralization and personal motivation, as anyone, anywhere can access this training without travel (Weimann, 2005). It is also interesting how terrorist organizations can actually capture information about the users exploring their websites, and then contact those users that seemed most interested based on their activity and possibly recruit. The Site Institute is a Washington, DC based terrorism research group that monitors al Qaedaôs activity, such as recruitment. According to Rita Katz, the Site Instituteôs director and author of the book *Terrorist Hunter,* she believes that, ñAl Qaedaôs use of the internet is amazing. We know from past cases ï from captured al Qaeda fighters who say they joined up through the Internet ï that this is one of the principle ways they recruit fighters and suicide bombers (Weimann, 2005). The Internet has become way too useful for modern day terrorists, but how do we go about making our insecure and vulnerable Internet secure?

Threat Prevention

Terrorism through the Internet is a major concern for national security. However, it is difficult to access the actuality of the threats and track the entire network of members involved. The Internet is a democratic institution, where anyone is able to post absolutely anything they wish. This freedom the Internet offers creates quite the obstacle for an intelligence analyst, who must determine: who they are ï why they are saying this ï is this person knowledgeable and credible - and do they have real motives (Lowenthal, 2012). However, the consequences of not regulating these threats are too high and dangerous to risk, which classifies this non-conventional terrorism as a low-risk/high-consequence threat (Shahar, 2005).

Prevention requires a multilayered approach, referred to as ñdefense in depth.ò The layers of this defense include policies and procedures, awareness and training, network segmentation, access control measures, physical security measures, system hardening, system monitoring, and antivirus sophisticated procedures (Franceschetti, 2011). Without proper security through these defenses, our society is in complete danger, even from the possibilities of false news of danger as the media today holds such power and could easily become hijacked (Shahar, 2005).

Terrorism as a whole is then combated through two capabilities ï prevention and reaction. Prevention is executed through two different stages; the first one is to make the perpetrators believe that their actions hold no chance in facing our systems. The second stage is to actually halt their actions from effectively working. Reaction involves controlling the effects of a terrorist attack, through countermeasures and prevention from further similar acts (Theile, 2005). The countermeasures mentioned above are also carried out through collection (gaining information about an opponentôs intelligence collection capabilities), defensive (halting efforts by hostile intelligence services to penetrate oneôs services), and offensive (having identified an opponentôs efforts against oneôs own system, trying to manipulate these attacks either by turning the opponentôs agents into double agents or by feeding them false information that they report back home (Lowenthal, 2012). These strategies involve all of the modern day security technologies that are available at present. It must be stressed that threats against our systems will only increase requiring continuous development of our programs and technological capabilities (Theile, 2005).

It is also important to note that the United States and its ñFive Eyesò partners, Australia, Britain, Canada, and New Zealand work closely in intelligence partnerships and have an agreement not to spy on one another. Beyond this ñFive Eyeò agreement intelligence agencies are free to roam (Lowenthal, 2012).

Trust: Team for Research in Ubiquitous Secure Technology

Our modern and civilized society today depends on systems. These systems include: electricity, transportation, banking, telecom, and health care ï all requiring security intelligence (Franceschetti, 2011). The operation of these systems is orchestrated through these systems of systems, of wired and wireless transmission, and the sharing of information through computers and Internet capabilities. In order to protect this delicate operation we must prevent intrusions, detect attacks, limit damage, and operate through attacks. These needs must be addressed through the designs of these systems, which must be trusted to hold strong enough barriers to penetration, accurate intrusion detection, and the ability to fuse incident reports and deduce plans for warning and action, as well as continue to aid in an attack (Franceschetti, 2011). Our protection systems with Homeland Security also require information assurance and survivability, security with privacy, secure network-embedded systems or cyber physical systems, validated modeling, simulation, and visualization of critical infrastructures and their weaknesses, as well as public ï private partnerships for technology transition. Developers must place an emphasis on modeling as

it may determine both strengths and flaws within the systemôs design (TRUST, 2013). In order to implement these dire needs for a safe and productive America, the organization Team for Research in Ubiquitous Security Technology (TRUST) was created to do a coherent job of focusing on these needs (Franceschetti, 2011). TRUST focuses on the development of cyber security, science, and technology, and is formed by six universities. The team universities include: Berkeley, Carnegie Mellon, Cornell, San Jose State, Stanford, and Vanderbilt. This team of undergraduates, graduates, researchers, engineers, scientists, and professors, works to solve problems that are too large and complex for any one group to investigate. TRUST was established as a National Science Foundation Science and Technology Center and is working to address technical, operational, legal, policy, and economic issues affecting our security, privacy, and data protection as well as the challenges of developing these systems (TRUST, 2013).

TRUST was created in 2005, and since then has obtained success through security and privacy issues involving medical records, web authentication, end-user privacy, next-generation browser security, malware detection, improved system forensic techniques to combat online attacks, an increase in secure embedded sensor networks for large-scale applicants critical to the nationôs economy, energy, security, and health (Franceschetti, 2011). TRUST has also worked on application defenses for network-level intrusions and attacks, including compromised and malfunctioning legacy applications, viruses, worms, and spyware, laws and policies that combine market incentives regarding design, deployment, and configuration of systems with privacy, security, and trustworthiness goals, as well as techniques that ensure trustworthy hardware, improved software robustness, and an increase in the survivability of critical systems. These security improvements were conducted through studying three major US applications; financial infrastructures (telecommunications and e-commerce), health infrastructures (personal health records), and physical infrastructures (including the US power grid, transportation, oil, gas, and water). It has also been realized through their successes, that only a multifaceted structure, such as TRUST, may translate the resulted substantive multidisciplinary progress to vendors, infrastructure service providers, and end-users (individuals), government organizations, international partners, and others (Franceschetti, 2011).

TRUST is also approaching security through a science base perspective with hopes to leverage these views on todayôs system developers. Most of computer security today is ñprimarily reactive,ò as it simply functions to react in deploying defenses for known attacks. TRUST believes todayôs security should be ñproactiveò which is possible through developing systems in a principled way. Their principled system includes: mental tools for understanding how to expose trust assumptions intrinsic in a system and how different defense mechanisms relocate trust assumptions in that system; how to characterize security properties which improve enforcement mechanisms and verification approaches; what defense classes can support security properties; and what classes of defense can resist classes of attacks (TRUST, 2013). Shankar Sastry, who is the NEC Distinguished Professor of Engineering at University of California, Berkley, states, ñThe theme of the center is restoring trust to all infrastructures: physical, electronic, and information (Team Science, 2013).ò

TRUST also works hard to place graduate students in direct contact with leaders in cyber-security, as the TRUST education director Kristen Gates states, ñNot only are we helping to educate and inspire students but weôre also helping to energize and invigorate younger faculty that are bringing these cyber-security and technology issues into their classrooms at our partner institutions (Team Science, 2013).ò Overall, TRUSTôs main mission is to restore ñtrustò to all infrastructures and help organizations develop information systems with a privacy policy that

allows them to manage sensitive information correctly (Team Science, 2011). Homeland security hopes to extend this TRUST prototype towards further fundamental research areas (Franceschetti, 2011).

Department of Homeland Security

The Department of Homeland Security has also increased its own effectiveness and experienced successful endeavors in recent years by leveraging the resources of the ICE Cyber Crimes Center, as DHS has been involved in Internet investigations concerning identity and document fraud, financial fraud, and smuggling (DHS, 2013). DHS is constantly working on building a world-class cyber security team by hiring a diverse group of cyber security professionals. The team includes: computer engineers, scientists, and analysts, in order to secure the nationôs digital assets and protect against cyber threats to critical infrastructure and key resources (DHS, 2013).

In 2012, Secretary Napolitano announced a new initiative through the Homeland Security Advisory Council with public-private partnerships. This initiative called for the development of an agile cyber workforce across the federal government. The DHS has since then increased the cyber-security work force by 500 percent over the past two years. In order to improve effectiveness, DHS has also centralized its key cyber-security functions, including the U.S. Computer Emergency Readiness Team (US ï CERT) and the National Cyber Security Division (NCSD), under a single Deputy Under Secretary for National Protection and Programs. DHS has also deployed the EINSTEIN 2 capability ï which is an automated cyber surveillance system that monitors federal Internet traffic for malicious intrusions and provides near real-time identification of malicious activity. These actions are made up of 15 Departments and agencies and four Managed Trusted Internet Protocol Service providers, private internet service providers that assist federal agencies in protecting their computer, networks, and information. In 2009, DHS opened the National Cyber security and Communications Integration Center. This security center operates on a 24-hour watch and warning system, which serves as the nationôs principle organization for organizing cyber response efforts and maintaining the national cyber and communications common operation picture. The DHS also has vital partnerships with antivirus companies in order to take proactive measures to stop possible threats from reaching public and private sector partners by developing and sharing standardized threat indication, prevention, mitigation, and response information products with its partners. In 2011, the DHS Industrial Control Systems Computer Emergency Response Team successfully conducted 78 assessments of control system entities, helping businesses to identify security gaps and prioritized needed measures. The Department of Homeland Security, through its cyber-security measures continues to secure our networks through the National Cyber Incident Response Plan, which provides a framework for effective incident response capabilities and coordination between federal agencies, state and local governments, the private sector, and international partners (DHS, 2013). The Department of Defense is included in the Department of Homeland Security partnerships, and following the aftermath of 9/11 and the Iraq WMD issue, standards in intelligence analysis have gone through great lengths to codify and raise standards as the Intelligence Reform and Terrorism Prevention Act includes a number of standards for intelligence analysis, as well as the DNIôs office (Lowenthal, 2012).

The Federal Bureau of Investigation

Following 9/11 the prevention of terrorist acts against the United States and its people became the FBIôs ñcentral mission,ò as this was promulgated by then Attorney General John Ashecroft in 2002 (Deflem, 2010). This shift of attention in the FBI has caused the Bureau to raise

its intelligence capabilities, especially through the use of National Security Letters (requiring the recipients to turn over records and data pertaining to individuals, also includes electronic communications and credit information) as it increases surveillance operations. The FBI has also created several counterterrorism divisions, including: the FBI Terrorism Financing Operations Section, a Weapons of Mass Destruction (WMD) Directorate, and the Terrorist Screening Center, in order to maintain the U.S. Governmentôs Consolidated Terrorist Watch list. Inter-agency cooperation has also been promoted as a Foreign Terrorist Tracking Task Force where the FBI partners with other federal agencies, including the CIA, ICE (U.S. Immigration and Customs Enforcement), and the Department of Defense. The most important counterterrorism tool developed in these operations has been the Joint Terrorism Task Force (JTTF). These task forces are controlled by the FBI and are composed of agents from other law enforcement agencies, other federal agencies, and first responder organizations. This JTTF organization acts as the primary investigative force in the FBI, as it follows up on leads, gathers evidence, collects intelligence, makes arrests, and provides security for special events. Out of the 100 JTTFôs in existence, 65 of them were created after 9/11 (Deflem, 2010). Due to this increase in intelligence operations, some analysts have raised concern over the decreasing experience of new hires, as veterans continue to retire in this present day. However, this younger generation of new hires has a better handle on the technologic aspects of todayôs non-conventional terrorism (Lowenthal, 2012). The successful system of the TRUST organization proves that we should have confidence in our younger intelligence generation in the future years to come.

Policy Recommendations

This paper has examined and explained the immediate need for revised security operations as well as the current operations underway to address these concerns. However, new development technologies against counterterrorism are only part of the answer. Computer science professor Fred B. Schneider at Cornell University and chief scientist of TRUST believes, ñThe solutions to todayôs cyber-security ills or trustworthiness problems are not going to come only from the technical side or from the policy side of the house ï but rather, from both sides working together.ò Kenneth Birman, a computer science professor at Cornell and TRUST coordinator for knowledge transfer, shares similar views as he states, ñSometimes the answer involves changing the law instead of changing the technology (Team Science, 2013).ò The truth in the matter however, is that better technology might not be adopted unless users face incentives to do so by becoming more aware of the reality of cybercrime.

After considering these TRUST perspectives and analyzing all aspects of todayôs modern terrorism threats and intelligence information systems, the rational approach for ñusersò is one supporting policy recommendations that push for funding towards technological advancements in cyber-security and computer science initiatives. Funding and grants towards organizations like TRUST assure Americaôs step ahead the countries which continue to pose threats against us. In order for these systems to work it is recommended that United States users agree to a policy in the form of forced protection. If users agree to a system of security, then they must agree to use security software, or to provide security information when needed or requested. All of these components are necessary otherwise these efforts are rendered useless.

A major part of the solution also lies in the hands of todayôs current media. The majority of public knowledge concerning terrorism is communicated through international media outlets. When a terrorist attack occurs, the news media is the first responder ï releasing photos and reports on the detail and devastating destruction. The actions by the reports communicate the success of the terrorists directly to the terrorists themselves. The media would better serve its purpose to the public by only reporting on ñactivitiesò and ñawarenessò of these terroristsô organizations.

Reporting this way does prove difficult as the greater percentage of todayôs audience enjoys the entertainment factor ñmediaò provides. It also requires extensive and dangerous conditions of journalism to report on terrorist groups and the sincere interest of an audience to follow these findings. The public today tends to only become ñawareò when something tragic happens. News media then caters to societies demand by relaying the terrorists exact and intended message ï simply feeding into what the terrorist wants. If the media invested more time in the actual gradual activities of terrorists ï ñthe backstage activities,ò then the terrorists wouldnôt hold so much power over the viewing society from ñshockingò events or ñattacksò reported (Herren, 2005). Eric Herren, of the International Policy Institute for Counterterrorism, believes that it should become our responsibility to educate the media of their responsibility as first responders to terrorist attacks as he states, ñThe media can then be used and/or misused as part of terroristôs psychological operations (2005).ò

Terrorism should also be handled through the development of multinational special operational teams. These teams would include regional intervention units whoôd be the first on scene to stabilize a situation and prepare the field for take-over units in the event of a situation. With this it would be recommended to establish an international counterterrorism unit which would bring together the best counter-terror solutions from around the world. At the same time, we must establish international and transnational centers of excellence, and idea exchange networks much like the TRUST operations, but at an international level (Herren, 2005). Through the process of these cyber-security developments and policy making strategies, the public must be informed of their options and threats against them. The general public must be more informed of the influence terrorism plays on public policy, in so far as it actually causing the need for public policy creation. It is the general public that suffers from security checks and loss of privacy and the more educated they are about the threats against them, the better they can understand or oppose policy changes that affect their everyday lives (Herren, 2005).

It is also important to recognize the need for the preservation of ñculture within society.ò Homeland security needs to take care to preserve the countries values of culture, tradition, and freedom, as well as all of our accomplishments and advancements weôve been through as a nation. If these values are protected, then a greater ñunifiedò country stands against the threats of terrorism destroying our society. As stated before with recommendations through policy, education of these issues must be encouraged in order to preserve the culture that we understand exists in America and to preserve what we want in America (Franceschetti, 2011). We need to take caution in our homeland security measures and our fight against terrorism in order to be wary of not eliminating the freedoms that we have fought for.

Today, cyber-security measures are growing rapidly as the past three administrations have spent billions towards cyber-security threat systems. The CCI ï Computer Crime Control Industry is now worth an estimated 27 billion, and will only continue to grow with advancements (Yarr, 2007). We must remember that all of the systems that our society is composed of are made up of systems interconnected ï the failure of one will affect the rest ï and in order to live safely we must protect these critical systems (Fraceschetti, 2011). As more individuals are logging on every single day, and the motivations and ease to commit cybercrime is increasing, it is as important as ever for the United States to be both aware and prepared within our cyber environment and our Nationôs information infrastructure.

References

Baer, Martha, and Heron, Katrina, and Morton, Oliver, and Ratliff, Evan. *Safe.* New York, NY: Harper Collins, 2005.

Bolton, M. Kent. *U.S. National Security and Foreign Policymaking After 911: Present at the Re-Creation.* United Kingdom: Rowman & Littlefield Publishers, Inc, 2008

Department of Homeland Security. Cyber Security Results. Last modified July 15, 2013. http://www.dhs.gov/cybersecurity-overview .

Deflem, Mathieu. *The Policing of Terrorism: Organizational and Global Perspectives*. New York, NY: Taylor & Francis, 2010.

Franceschetti, Giorgio. *Homeland Security: Threats, Countermeasures, and Privacy Issues*. Norwood, MA: Artech House, 2011.

Herren, Eric. ñTools for Countering Future Terrorism.ò In *Countering Modern Terrorism,* edited by Knop, Neisser, & Creveld, 385 ï 396. Berlin: DE. W. Bertelsmann Verlag, 2005.

Kshetri, N. (2013). ñCybercrime and cyber-security issues associated with China: some economic and institutional considerations.ò *Springer Science + Business Media,* (2013):1 -29.

Lowenthal, M. *Intelligence: From Secrets to Policy*. United Kingdom. SAGE Publications Ltd, 2012

New Media Institute. *History of The Internet.* Last modified 2012. http://www.newmedia.org/history-of-the-internet.html

Shahar, Yael. ñNon-Conventional Terrorism: Challenge & Response.ò In *Countering Modern Terrorism,* edited by Knop, Neisser, & Creveld, *361* ï 370. Berlin: DE. W. Bertelsmann Verlag, 2005.

Team Science. ñTeam for Research in Ubiquitous Secure Technology.ò Last modified 2013. http://depts.washington.edu/teamsci/pdfs/_TeamScienceTRUSTPg52-55.pdf

TRUST. ñThe Team for Research in Ubiquitous Secure Technology.ò Last modified May 2013. http://www.truststc.org/index.html

Theile, Burkhard. ñTechnologies against Terrorism.ò In *Countering Modern Terrorism,* edited by Knop, Neisser, & Creveld, 407- 415. Berlin: DE. W. Bertelsmann Verlag, 2005.

Weimann, Gabriel. ñHow do Terrorists use the Internet?ò In *Countering Modern Terrorism,* edited by Knop, Neisser, & Creveld, 87-109. Berlin: DE. W. Bertelsmann Verlag, 2005.

Yar, Majid. ñComputer crime control as industry: Virtual insecurity and the market for private policing.ò In *Technologies of Insecurity: The Surveillance of Everyday Life.* Edited by Aas, Gundhus, & Lomell, 189 ï 200. New York, GlassHouse, 2007.