Running head: Combating Terrorism

Combating Terrorism

SGM Lawrence E. Andrews, Jr.

MSG Cheryl Greene

SGM John Rek

SGM Wayne Fausz

United States Army Sergeants Major Academy

Class # M05 – Team A

CMDCM Cain

27 November 2007

Outline

I. Abstract

II. Introduction: Combating Terrorism

III. Border Security

- A. Border and container security
- B. Policies and programs
- C. Costs and challenges
- D. Illegal immigration

IV. Airline Security

- A. Cargo Screening
- B. Passenger Screening
- C. U.S. Air Marshals

V. Law enforcement

- A. Public safety and terrorism
- B. International law enforcement cooperation
- C. Terrorism – Past, Present and Future
- D. The global challenge

VI. Infrastructure

- A. Energy plant security
- B. Chemical plant security
- C. Water supply
- D. Cyber Warfare

Abstract

On September the 11th, 2001, radical Islamic terrorists proved that the United States was unprepared for terrorist type attacks. Since then the government has gone to great lengths to secure its borders, airlines, infrastructure and improve it's law enforcement abilities. Massive sums of money have been spent in each of these areas with mixed results. Training has been expanded and agencies are now working together that never did before the attacks. Weaknesses that were completely unknown are being addressed. Yet, while the country is much safer today than six years ago, the United States must continue to improve current programs while utilizing all resources to ensure that systems are in place to prevent future terrorist attacks.

Combating Terrorism

September 11th, 2001 was viewed as very much the modern day Pearl Harbor sneak attack on the American public. We were caught off guard. Americans did not think it could happen here on American soil. Thinking that, the government and the American public had done little to persuade terrorists otherwise. Following the attack the public outcry to find out what happened was tremendous. This also caused the government to scramble and put preventive measures in place to thwart any possibility of another attack. Since then, the Homeland Defense Department has been created and legislation and rule written. While many steps have been taken, there are many more that need to be implemented. The United States Government has failed to invest enough time, money, and manpower to successfully combat terrorism in the areas of border security, airline security, law enforcement and infrastructure security.

Border Security

A safe country is the one, which is not entered by illegal aliens and even worse by terrorist. To be able to prevent the entry of illegal aliens and terrorist to the United States, international borders should be secured. The United States Border Patrol (USBP) is responsible for the protection of the country's borders. Today, their primary goal is to spot and prevent the entry of terrorist groups, illegal aliens, weapons of mass destruction, drug and human smugglers, and criminals.

USBP is now under the Bureau of Customs and Border Protection (CBP), which is administrated by the Directorate of Border and Transportation Security (BTS). This adjustment was brought on by the Homeland Security Act of 2002 to enable better protection of the international borders of the United States. As already stated, the role of the USBP is to prevent entry of terrorists, illegal aliens, weapons of mass destruction and to stop any act of smuggling or

drug-related businesses between official points of entry. The USBP does not run the points of entry. Agents from the Bureau of Customs and Border Protection are the ones responsible for the immigration, customs and agricultural transfer of products (CRS Report for Congress, 2005).

Border Patrol and Container Security

Great responsibility is designated to the USBP. They have to manage and train the necessary manpower while ensuring correct use of current technology for the protection of the international borders. These extend from the northern border (Canada) to the Southwestern border (Mexico) and include the coastal waters around Florida and Puerto Rico. The Southwestern border differs in geography, length and number of migrants than that of the Northern border. Although, the length of the Mexican border is half that of the US-Canadian border, it has by far had the most number of illegal immigrants crossing. The USBP has managed this problem by sending most of their manpower to the Southwestern border. Apparently, the same degree of threat is present within the US-Canadian borders; it is more evident that terrorism might inflict harm due to the length of the border. Due to these issues, the USBP is focusing on technology. They have installed detection equipment at ports of entry and on unfenced sectors of the boarder to help monitor the entry of any kind of terrorism-related activities (CRS Report for Congress, 2005).

On the other hand, the Bureau of Customs and Border Protection (CBP) initiated the Container Security Initiative (CSI) in 2002. The main goal of the program is to amplify the security of the container cargo, which is shipped to the US.

Policies and Programs

After the 9/11 attacks, the government through the USBP has refocused its mission on preventing the entry of any terrorist and weapons of mass destruction. They formulated the new

National Border and Patrol Strategy in March 2005, which exhibits great concerns on terrorism-related activities. They continually develop technologies that will improve the security of our borders. Among those developments is the America's Shield Initiative, which integrates the Remote Video System (RVS) camera system and the Integrated Computer Assisted Detection (ICAD) database to a multi-faceted network, which has the ability to detect the illegal entries in various climate conditions. They also continue to use the Automated Biometrics Identification System (IDENT) to identify and track illegal aliens (CRS Report for Congress, 2005).

The Container Security Initiative (CSI) was also a program developed for the purpose of protecting threats from terrorism. This was initiated by the CBP to uphold the security of the container cargo.

Cost and Challenges

The harms that the American government is now facing are still numerous. Today terrorist networks are even more isolated. Many countries from all over the world have been attacked without prevention it all. The terrorists are planning to use weapons of mass destruction. These are among those threats and problems that are faced by the United States. Aside from these, protecting the borders and ports of the country is still a big responsibility due to the sheer size of the task. The Bureau of Customs and Border Protection total budget allotted for 2007 is $7.84 billion, an increase of $702.31 million from 2006. With this budget, they expected that they will perform their responsibility and will surely protect the borders and ports of America from any harm (US Customs and Border Protection, 2006).

Illegal Immigration

There are approximately 12 to 15 million illegal aliens in the U.S. Every year there is an increase in the rate of illegal immigrants sneaking across the borders of the country (BBC News,

2006). This threatens the security of the country because of the probably of entry of terrorists or any criminal aliens. Moreover, due to this number, the government of the U.S. is expediting technology development and employment, manpower increases and all necessary resources to ensure the safety of the homeland from any harm or threats.

Airline Security

Before 11 September 2001, American airline passengers were able to travel freely throughout the United States by commercial airlines. Airport security was nearly non-existent. Americans didn't have to worry about arriving early at the airport to go through stringent security checks. Americans were able to roam freely throughout the airport; hand carry items onto planes, and family members were able to accompany loved ones to the airplane. Since 11 September 2001, American airports have been mandated to increase their security procedures. Transportation Security Administration (TSA) increased their security procedures by implementing strict passenger and cargo screenings. U.S. Air Marshals began flying on numerous randomly chosen flights. Passengers were restricted to certain areas of the airport. Passengers are also restricted from hand carrying certain items on commercial airlines, and families are unauthorized to accompany loved ones to the airplane.

Cargo Screening

Since the terrorist attacks on 11 September 2001, the number and types of equipment for screening cargo has grown dramatically. The use of X-ray and gamma ray machines has tripled since the attacks. All airports are required to use these types of technology to scan air cargo that accompany passengers on aircraft. Each day more than 50,000 tons of cargo is transported by air. According to a TSA report to Congress "While a great majority of this cargo is placed on cargo-only aircraft, 26 percent is transported in passenger planes" (Transportation Security

Administration, 2006). Transporting air cargo is an important source of revenue for air carriers and our economy. Before the terrorist attacks cargo stored in the cargo bays of passenger aircraft were never inspected for hazardous materials. Post 9/11, Transportation Security Administration was mandated by the Homeland Security Committee to employ a multi-layered security system in air cargo areas. TSA has since strengthened the entire security system and introduced unpredictability that the system can't be manipulated. TSA now only allows known shippers to ship cargo on passenger aircraft. Canine units have been incorporated throughout the cargo areas. TSA screens all cargo with electronic explosive detection systems and they mandate that their inspectors' conduct scheduled and unscheduled inspections on random cargo. High-risk cargo is inspected 100% before being placed on any passenger aircraft. All cargo is eligible for screening without exception or consent. By incorporating these procedures and other counter measures, TSA ensures the security of their passengers. TSA continuously evaluates possible potential enhancements to ensure cargo security. There are two major factors that hinder the inspection of cargo and the security of airline passengers. First, funding is an on going battle with the Homeland Security Committee. TSA requires additional funds for security; the Homeland Security Committee is not willing to commit to the additional funds. Second, the X-ray machines and the gamma ray machines are bulky and susceptible to environmental exposure and mechanical breakdowns. Maintenance and care for the security machines is becoming very costly.

Passenger Screening

Since 11 September 2001, TSA has intensified their passenger screening. Law mandated that TSA thoroughly screen air passengers to ensure that prohibited items and undesirable passengers don't board commercial airliners. TSA screens millions of bags and passengers for

contraband and other explosive devices each day. As a result of the mandate, TSA now has over 7,200 baggage screening locations at over 450 airports nationwide. TSA states in its web site, "We are most visibly present through our 43,000 trained and certified Transportation Security Officers stationed at over 450 airports across the country" (Transportation Security Administration, 2006). Due to 9/11, TSA was also directed by the Secretary of Transportation to associate with the Department of Homeland Security's Technology Research Lab for research and for using modern technology. Through rigorous research, TSA has fielded the latest sophisticated technology to screen all passengers and luggage. TSA is constantly fielding the latest products and regulations. This allows the newest technology to be implemented for both checked baggage and passengers. Technologies, such as X-ray machines, body scan machines, computer enhanced screens displays, and explosive trace detectors have helped TSA inspectors to deter violators of airport security. TSA also states in its web site "In an airport security test, between October 2001 and January 2002, TSA inspectors overlooked 65% of the knives, 25% of the guns, and 55% of the test bombs in passenger's luggage. In the same security test, smugglers were successful in smuggling makeshift bombs through TSA security 20 of 20 times" (Transportation Security Administration, 2006). TSA is working diligently to train their inspectors on a regulator basis and supply them with the latest technology. Screening will never be perfect, but illegal items such as knives, guns and bomb making materials should never escape our TSA airport security.

U.S. Federal Air Marshals

The U.S. Federal Air Marshals Service serves as the number one security agency in the TSA. Before 11 September 2001, there were only 50 U.S. Air Marshals who flew on solely international flights only. After the terrorist's attacks in September 2001, the Secretary of

Transportation expanded the U.S. Federal Air Marshal program. With the directive, U.S. Federal Marshals began flying around the world and on United States flights. “As a result of the attacks, President George W. Bush ordered the rapid expansion of the Federal Air Marshal Service. Over 200,000 applications were initially received, from which several thousand qualified Federal Air Marshals were selected. Those who were hired came from a diverse background of experience including other federal, state, and local law enforcement agencies and the military” (Homeland Security, 2006). As a result of 9/11, the U.S. Federal Air Marshal Service pre-positioned twenty-one field offices in and around our nation’s airports. There are several hundred of the Assistant U.S. Federal Air Marshals stationed directly at airports in the United States. There are also U.S. Federal Air Marshals attached to each of the fifty-six Federal Bureau of Investigation (FBI) Joint Terrorism Task Forces nationally. The U.S. Federal Air Marshals play a major role in homeland security since the terrorist’s attacks. They continue to work indefatigably with public and local security forces to deter security violators and to promote a safe and secure atmosphere for passengers. As of now, the U.S. Federal Air Marshals serve in various staff assignments and positions at organizations like the National Counter-terrorism Center and the National Targeting Center. U.S. Federal Air Marshals are in-bedded with local law enforcement and liaison assignments in an alert crisis and during national holidays. By directly placing U.S. Federal Air Marshals strategically throughout the United States, they are able to quickly respond to changing security threats as they occur. U.S. Federal Air Marshals are trained to high standards and they train on a daily basis to maintain those standards. U.S. Federal Air Marshals have the highest firearms qualification requirements in law enforcement.

Law Enforcement

America is fighting for its values and way of life in the Global War on Terrorism (GWOT). There are many countries that have supported the United States in the battle, which pits radical Muslims against Western Civilization. Not only American Soldiers, but also Soldiers of other nations are risking their lives for freedom. The police and other agencies responsible for enforcing the law must secure innocent civilian lives and their property. For the last six years, law enforcement forces have received more money and personnel than ever before. They must use these resources wisely to keep our world safe against terrorism.

Public safety and terrorism

Terrorism poses a serious threat to individuals' lives and national security around the world. We all must help keep the nation and public safe from terrorism. The police forces of America are working diligently to solve the problem of extremist born and raised here in the United States, while responding rapidly to their criminal acts. The method of pursuing dealers, fiscal service sources, and financially interested parties means that single illegal incidents are often not isolated incidents, but are often an integral element of a series of connected offenses. Local authorities must handle native extremists and the felonies they commit right in their backyards. Nationally run law enforcement components must guarantee that local police services have a clear and extensive picture of domestic extremists. This will provide local police with a clear representation of the criminals they are facing. (Public Safety and Terrorism, 2007). The authorities will be responsible for investigating events at both local and national level. Being proactive in their duties will lead to convictions in the criminal courts. It is imperative that we bring the efforts of all our law enforcement agencies together because if the terrorists decided to

"smuggle a nuclear weapon into New York City there is almost nothing anyone could do about it" (Evans, 2007, p. 166).

International law enforcement cooperation

The Federal Bureau of Investigation (FBI) and the Central Intelligence Agency (CIA) correspond with intercontinental law enforcement entities and police units in other nations, such as Interpol, to distribute intelligence and the newest methods on combating radical transgressions against domestic targets. The task is to aid global law enforcement collaboration linking the United States with the International Criminal Police Organization (INTERPOL) as well as other worldwide police forces. Interpol currently includes 186 member countries.

Interpol has made accessible a variety of assets to assist all associate nations with their challenges to safeguard their societies from terror campaigns. Interpol maintains items of information, conducts investigations and provides intelligence concerning targeted individuals and factions, and their actions. The institute also coordinates warnings and pertinent information on terrorists, suspected criminals and threats to law enforcement agencies in affiliated countries. An example of this cooperation is the Fusion Task Force, created after the September 11 assault on the United States. Interpol now issues realistic courses of action on the type of information required to hunt down and prosecute international and domestic terrorists. Associate nations are strongly encouraged to provide information on other crimes however insignificant they may seem, because there is a chance, the crimes are coupled to terrorism. Examples of seemingly unrelated crimes are suspect monetary transactions, arms trafficking, phony travel and identification papers, and the capture of nuclear, biological and chemical producing materials. The growing likelihood of terrorists attacking with biological or chemical weapons is a particularly pressing anxiety for all peace-loving nations of the world. Enforcing the law should

be more effective these days. Worldwide support must center on enhanced synchronization of investigation; identify involving patterns and trends of illegal activities, exchange information and share analysis as well as knowledge (U.S. National Central Bureau of INTERPOL, 2007).

Terrorism – Past, Present and Future

Concern about terrorism has never been greater than in the past few years. There is new evidence that seems to prove unrelated incidents now tie chance criminal acts to a wave of international violence and terrorism. In the pre 9/11 days, most acts of terror were somehow politically motivated; however today there is a cornucopia of groups with different agendas and demands. Terrorist attacks can occur anywhere in the world. It has happened and it will probably happen again. A terrorist attack is so brutal and random that it shocks the mind of the victims and the citizens of the country in which it occurs. This kind of attack is more powerful than all other criminal acts. Small groups, inspired by a new brand of fatalism, are carrying out the actions of the "new terrorist."

Law enforcement units must improve their critical analysis when determining where the current threats to our country and the world really exist. Uncovering the threat is becoming more difficult than ever before because there are no obvious borders to cross and there are very few patterns in which to dissect. Organized structures are becoming more difficult to smoke out, because members who move with the refugee and immigrant populations carry the terrorist messages all over the word. These messages are coded and hidden into family events and salutations, which make them evermore challenging to decode for the world's counter terrorism officers. It is imperative that federal and state officials work closely together to monitor suspect groups and individuals without missing a person of interest or duplicating efforts. In the international arena, the intelligence services must call for bilateral accords, which will assist

prosecution, rather than promoting costly military operations. The key to preventing a terrorist act is intelligence, which is represented by the cooperation, and synchronizing of the FBI, CIA, and Interpol as well as Local/State agencies efforts (Perry, 2007).

The global challenge

Terrorism is a global problem. The actions of the recent years have proven that the international danger of terrorism has not lessened and that the most significant menace to our lives is that offered by radical fundamentalist (such as Al-Qaeda and like – minded groups). In the recent past, no area of the world has been spared the atrocities of modern terrorism. Terrorism is most certainly a universal threat to humanity. No problem we face in the 21st century is as important to solve. To reduce the danger and guard the lives of people around the world, global administrations and law enforcement agencies must work together to capture known terrorists, and avert future terrorist activities. Increased security measures to prevent terror do not and should not warrant a breach of personal and civil liberties. If we rob our citizens of their rights in pursuit of the terrorists, the criminals have won by default. Only the future will give us an answer to this question. Terrorists have demonstrated the aptitude necessary to adjust to law enforcement efforts to incarcerate them.

There are two limitations to worldwide law enforcement collaboration, which destabilize its success. The first limitation is geographical in nature and the second is functional in nature (Noble, 2004). International conventions and accords center on legal collaboration rather than on law enforcement teamwork. Every nation has a duty and an obligation to their citizens to stop dangerous criminals from entering their country. Currently this is not happening today in an efficient manner due to different standards around the world. Countries have a responsibility to warn other countries about individuals that present a potential danger. Nations must make certain

that information about subjects, sought for terrorism and or other crimes are immediately entered into international databases. Police must possess the equipment to speak globally with one another without excluding any state. Countries have a duty to provide information on any internationally pilfered papers. It is vital that states distribute information about passports that are reported stolen, because documents such as these are indispensable tools for terrorists. Global sharing of data in passports, national identity cards, and visas is not occurring at the level it should. Every country should have a police office, staffed 24 hours a day 7 days a week, which can immediately query international databases, respond to urgent information requests from police officers in the field and act on information, received from other states, in real time.

Countries must ensure that their police forces are properly trained. All of the world's nations should attempt to reach a consensus and cooperated towards their useful realization, rather than focusing only on the harmonization of penal law or the creation of new institutions. Committing to these principles will help the international community making the world safer for it's citizens (Noble, 2004).

Infrastructure

Before the September 11th attacks, little thought was given to the security of America's infrastructure with the exception of protecting nuclear power plants. Most Americans failed to look outside the box. They did not want to take a look at the perceived little things that could cause a major disruption in our way of life. No one considered a plane flying into a nuclear plant. No one thought about the poisoning of a major water system. Certainly few measured that taking out the Internet would cause an immense economic impact, not only within the financial system, but to everyday people as well. Since then, much has changed. Our citizens have demanded that the government respond and it has. To increase the security of our infrastructure, the government

has spent immense money and dedicated uncounted resources to shore up their safety. December 2003, the *Homeland Security Presidential Directive 7* was issued to establish policy directing the protection of critical infrastructure. This policy required the protecting of those things that make life in the United States what it is. This was deemed CIP, or "critical infrastructure protection." Let's take a look at some of the steps taken to protect the infrastructure of the United States (*What is CIP and why is it important?*, 2003).

Energy plant security

The capture or destruction of an energy plant would be a major victory for terrorists, as it would bring enormous publicity to their organization. America has multiple energy plants scattered through out the United States. Most of these plants are coal or natural gas powered and would do little other than cut electricity to homes and businesses if captured or destroyed. Any fire set to the energy plant would most likely be put out quickly and the pollution minimized. However, there are 103 nuclear reactors at 64 different sites in 31 states (Butcher, 2006). When we look at the effects of a possible terrorist attack on these, we see that the results have much more potential to inflict damage. While an explosion is unlikely, a meltdown or fire at a nuclear reactor could spread radiation over a large area. We know that Al Qaeda has been looking at this possibility. In 2002, President Bush told the world that American Soldiers "found diagrams of American nuclear power plants" in Afghanistan (Butcher, 2006). Because of this information, the events of 9/11, and the creativity of the terrorist, the government has taken steps to improve security around all of our plants.

The Nuclear Regulatory Commission, or NRC, has had oversight of our nuclear plants since 1975. They have ensured the plants run correctly and safely, that people are trained, and they put in place the requirements for security of each plant. Before 9/11, the commission had

stringent safeguards to prevent attacks on the plants. This included barriers, fences, intrusion detection systems and armed guards. However, since that time they have issued orders that significantly strengthen the plants. The NRC has ordered plant owners to strengthen the physical barriers for a larger foe than expected previously. They now require stricter control of access for entrance and the inspection of vehicles at a further distance from the plant. The NRC has forced better coordination between local, state and federal response agencies to include the planning process for an emergency. Additional communications have been put in place between our intelligence organizations, our military and the plants. The NRC has ordered the plant owners to upgrade their ability to react to fires or explosions and to increase the training and qualification of plant security. Finally, the NRC has developed a better force-on-force program to test security (Butcher, 2006).

On the surface, it appears that much has been done to improve our Nuclear power plant safety. Yet many critics say enough still has not been done. According to an article by the Associated Press, plants had been required to plan for an attack by a force of only four people to include an inside source. This requirement has been doubled since 9/11. Expressing concern that the upgraded defense plan falls well short, attorneys general from seven states — which together have 31 of the nation's 103 commercial power reactors — wrote the NRC last year saying that the agency "should require defense attacks […] by groups at least as large as that involved in the 9/11 attacks" (Butcher, 2006). These arguments go against a highly classified report and leave many questions for the public. Has enough been done for our power plants? The industry will tell you that 1.2 billion dollars has been spent on upgrades. The real questions are, "Were they the right ones?" and "Are they enough?"

Chemical Plant Security

Probably the most dangerous of all potential targets in America are our chemical plants. There are over 15,000 separate plants located throughout the U.S. Many of these plants have the potential to kill thousands. According to the Department of Homeland Security, one individual exploded chlorine tank has the potential to kill 17,500 people, seriously injure another 10,000, and hospitalize up to 100,000 (Wayman, 2005). While the American Chemistry Council (ACC) has established a guideline that its members are required to meet, the association consists of only 2,000 of those plants. In 2003 alone, the ACC claims that it's members spent over $800 million increasing security and hardening its plants (Wayman, 2005). This leaves 13,000 plants to worry about. Finally, in 2007, the Department of Homeland Security got a bill passed that places requirements on all the chemical plants in America. This is only six years after the attacks of 9/11. The bill is only an interim bill, but it does require vulnerability assessments and the development and implementation of security plans (DHS Chemical Facility Anti-Terrorism Rule Provides Structure, Penalties, pg. 1). As one can see, this has been a weak point in the Homeland Security's shield to protect Americans. What remains to be seen is if the final requirements will be enough and will they be in place before the terrorists attempt to exploit the vulnerability.

Water Supply

The Environmental Protection Agency (EPA) has the lead on all matters concerning our water supply, to include anti-terrorism. Before 9/11, little was done to prevent terrorism with our water supply. Most of the concern about water was centered on ensuring that it was your usual safe to drink. No one thought about someone actually trying to poison people through the water supply. Nevertheless, according to J.M. Kalil and Dave Berns of the Review-Journal, that is exactly what the terrorists were trying to figure out how to do. Their article, *DRINKING*

SUPPLY: Terrorists had eyes on water, says that they (the terrorists) knew that they couldn't contaminate a water source, as it would dilute contaminates too much. However, they were looking into contaminating the water through a treatment facility. All this information was discovered in a federal bulletin released in 2004. This is just one of the things the EPA is trying to guard against. This is an especially hard endeavor as every town has a water source and each must be protected.

Following 9/11, the EPA required all water treatment facilities conduct vulnerability assessments. The EPA has provided grants to help with the assessments, technical assistance, and training required on homeland security issues. In 2007, the EPA is providing over $5 million to states to help with water issues. These funds are to help in the start of security enhancements, to train on emergency plans and response, developing redundant and mitigating plans along with supporting agreements between different water companies to support each other in times of disaster (U.S. Environmental protection Agency, 2007). What is most interesting is the EPA decentralized the program and monies so that states could do what they saw best, yet with guidance. Additionally, the EPA ensured that the states work on the largest facilities first, with the intent to go back and upgrade the smaller systems over time.

The EPA has a comprehensive plan that is spreading the wealth between both the large and small water systems. They have established environmental training centers to focus on vulnerability assessments, security upgrades and emergency plans. It appears that the government is taking all the right steps, while not complete, to secure our water systems and protect against an attack on our most precious resource, water.

Cyber Warfare

In the last 30 years, computers have revolutionized the way we live. We have come to depend on them for everything from paying bills, to communication, to calculating payrolls for the local business. Yet, this is also one of our biggest vulnerabilities. Imagine waking up tomorrow and finding that you will not be able to use your credit or debit card for a week or two. A week later, the local grocery stores are running out of the most used food. Unfortunately, the server they sent the orders through was knocked out and is expected to stay that way for a couple of more weeks. While it sounds far fetched, it's not.

According to James Lewis, a researcher at the Center for Strategic and International Studies in Washington, D.C., "There's a vulnerability in every system. If it's not a faulty firewall or an unprotected mobile device, it can be as simple as an employee's password written on a yellow post-it note" (Greenberg, 2007). Hackers can get into just about anything. It is just a matter of time and creativity. In some cases, it can bring a whole country to its knees. In May of 2007 the Estonia government decided to move an old USSR memorial. This made the Russian population very upset. Many protested the move by marching. However, the hackers protested by computer. They issued denial of service notices through multiple computers, which they had taken over using hidden software. This caused banks, media and government computers to go down, many for over a week (Greenberg, 2007). Imagine if those hackers had the government's backing (which Estonia could not find) what they could have done. Well, it's not that hard. In September of this year, the Financial Times reported that the Chinese had hacked into the Pentagon computer system (Several countries trying to hack into US military system: Pentagon, 2007). While the American government will not admit anything publicly other than the Secretary of Defense's e-mail had been breeched, one can read between the lines. It seems almost monthly

there is another announcement that a commercial system was breeched, but now we are also concerned about our government and military computers.

Finding information showing what is being done to stop this kind of terrorism is difficult at best. However, in October of 2007 the U.S. Air Force announced the creation of a cyber command. This seems like a step in the right direction. Yet, even the U.S. Air Force Chief of Staff Gen. Michael Moseley, has stated, "The United States is late to the fight" (Waterman, 2007). The question becomes, is this going to be enough? In September 2007 in Geneva, world experts came together to see if they could start helping with the problem. America has got to get in this fight either by itself or together with the world. It will be interesting to see if the cyber command along with good old capitalism will be able to stop the terrorists when the time comes. The Air Force knows that the civilian community has the ability to protect against cyber-terrorism and we can implement most of it, however do we have the national will to do so? Do we execute the politically incorrect thing such as take down a pro-terrorist web site that is causing harm to the United States or allow the world to have the same freedom of speech we have here. Unfortunately, only time will tell on this one.

Conclusion

September 11th 2001 is a day that changed the United States forever. The events of that day affected the way our country thinks. It completely changed Americans opinion of what the government must do to keep them safe. Consequently, the government has stepped up to the plate and has taken on the major challenges that are necessary to ensure another attack does not stop the way we live. However, our intelligence and law enforcement agencies must share all information with one another and take advantage of emerging technology. The government must improve and expand its investment on technology on the boarders. TSA has to continue to

upgrade their security procedures and require their personnel to adhere to the standards set fourth by the Department of Homeland Security Committee. Rules and regulations must continue to be refined in all areas to include infrastructure, while ensuring that training is realistic and tough. While the United States Government has invested an immense amount of time, money, and manpower to combat terrorism in the areas of border security, airline security, law enforcement and infrastructure security, there remains much that needs to be done to complete the process.

References

BBC News (23 May 2006). Viewpoints: US illegal immigration. Retrieved November 6, 2007 from http://news.bbc.co.uk/1/hi/world/americas/4989248.stm

Burns, D., Kalil, J.M., (2004). *Drinking supply: Terrorists had eyes on water*. Retrieved October 16, 2007, from http://www.reviewjournal.com/

Butcher, D. (2006). How vulnerable are U.S. power plants? ThomasNet.com. Retrieved October 19, 2007, from http://news.thomasnet.com/IMT/archives/2006/02/how_vulnerable.html?t=archive

DHS Chemical Facility Anti-Terrorism Rule Provides Structure, Penalties. (2007.) Retrieved October 16, 2007, from http://petrochemical.ihs.com/news-07Q2/dhs-chemical-facility-anti-terrorism-rule.jsp

Evans, M. (2007) *The Final Move Beyond Iraq*. Lake Mary, Florida: Front Line Publishers.

Greenberg, A., (2007). Business of fear. Retrieved October 29, 2007, from http://www.forbes.com/2007/10/26/tjx-northrop-mcafee-ent-tech-cx_ag_1026worsthacks_slide_2.html?thisspeed=20000

Homeland Security. (2006). *Homeland security law enforcement*. Retrieved November 9, 2007, from Homeland Security: http://www.tsa.gov/lawenforcement/mission/index.shtm

Neto, Blas, & Nuñez (2005). CRS Report for Congress. Retrieved November 6,2007 from http://www.fas.org/sgp/crs/homesec/RL32562.pdf

Noble, P. (2004). *Prosecuting Terrorism: The Global Challenge*. Retrieved October 12, 2007, from http://www.interpol.int

Perry, S. (2007). *Terrorism: A Frightening New Perspective*. Retrieved October 12, 2007, from http://www.totse.com

Public Safety and Terrorism. (2007). Retrieved October 12, 2007, from http://www.interpol.int/Public/Terrorism/default.asp

Several countries trying to hack into US military system: Pentagon. (2007.) Retrieved on October 22, 2007 from http://www.spacewar.com /

The White House. (2006) Retrieved November 6, 2007 from http://www.whitehouse.gov/nsc/nsct/2006/sectionII.html.

Trasnportation Security Administration. (2006). *Department of Homeland Security*. Retrieved November 15, 2007, from TSA.GOV: http://www.tsa.gov/research/asac/index.shtm

Transportation Security Administration. (2006). *TSA.GOV*. Retrieved November 05, 2007, from Homeland Security: http://www.tsa.gov/what_we_do/tsnm/air_cargo/index.shtm

US Customs and Border Protection (2006). President Bush's FY 2007 budget for U.S. Customs and Border Protection (CBP) totals $7.8 billion. Retrieved November 6, 2007 from http://www.cbp.gov/xp/cgov/newsroom/fact_sheets/budget/bush_2007_budget.xml

U.S. Environmental Protection Agency. (2007). *Grants and funding.* Retrieved October 19, 2007, from http://cfpub.epa.gov/safewater/watersecurity/financeassist.cfm

U.S. National Central Bureau of Interpol. (2007). Retrieved October 12, 2007, from http://www.usdoj.gov/usncb/usncborg/mission.html

Waterman, S., (2007). Analysis: A new USAF cyber-war doctrine. Retrieved October 22, 2007 from http://www.spacewar.com /

Wayman, B. (2005). Protecting chemical plants from catastrophic failures, part 1. SecurityInfoWatch.com. Retrieved 17 October, 2007, form http://www.securityinfowatch.com/article/article.jsp?siteSection=371&id=2908

What is CIP and why is it important? (n.d.). Retrieved October 18, 2007, from U.S. Fire Administration Web site: http://www.usfa.dhs.gov/fireservice/subjects/emr-isac/what_is.shtm

Public Safety and Terrorism. (2007). Retrieved October 12, 2007, from http://www.interpol.int/Public/Terrorism/default.asp