2008

Running Scared of SCADA: An Analysis of the Vulnerabilities of America's Infrastructure to a Cyber Attack

Ryan Tesnow

Follow this and additional works at: http://digitalcommons.unf.edu/ojii_volumes

Part of the Social and Behavioral Sciences Commons

Running Scared of SCADA: An Analysis of the Vulnerabilities of America's Infrastructure to a Cyber Attack

Ryan Tesnow
Faculty Sponsor: Dr. Paul Harwood

Abstract

  Cyber terrorism is the new ever evolving enemy of our future. Its impact on Supervisory Control and Data Acquisition (SCADA) systems, which function within all America's physical and cyber infrastructure, is so complex and perilous critical action must be taken. Over 75% of the world's oil and gas pipelines are monitored and controlled by SCADA systems (Lewis 229). Factor in that almost 78% of internet attacks are traced overseas we must be aware of the 1.2 billion internet users worldwide (Verton). With over 5,000 airports, 3,000 government facilities, 104 commercial nuclear power plants, 5, 800 hospitals, 8,000 dams, and over 1,600 wastewater facilities we are all slaves to electrical power and in turn, the reliability of our cyber infrastructure (Verton). However, our biggest risk may lay in the fact that over 85% of our infrastructure is owned privately where cost efficiency flies high above systematic security. In my study I conducted more than ten interviews with high ranking government officials and also cyber security analysts. The hypothesis that our physical and cyber infrastructure are in critical danger was strongly supported by my research. Fundamentally, as technology continues to expand and systematic security becomes more necessary we must be skeptical of those that find solace in solely cost efficient initiatives.

Introduction

  At issue in this paper is cyber terrorism and its impact on the Supervisory Control and Data Acquisition (SCADA) systems that function within all America's physical and cyber infrastructure. Over 75% of the world's oil and gas pipelines are monitored and controlled by SCADA systems (Lewis 229). Also more than 1,700 of our countries 2,800 power plants use SCADA systems to run their electrical substations (Lewis 229). In the United States alone there are a total of 170 million personal computers and of our population of 334 million people, 234 million are believed to be internet users ("Internet World Stats"). However, this figure does not do justice to the true physical state of affairs. With almost 78% of Internet attacks being traced overseas we must factor in the worlds over 1.2 billion internet users (Verton). With over 5,000 airports, 3,000 government facilities, 104 commercial nuclear power plants, 5, 800 hospitals, 8,000 dams, and over 1,600 wastewater facilities we are all slaves to electrical power and in turn, the reliability of our cyber infrastructure (Verton). However, our biggest risk may lay in the fact that over 85% of our infrastructure is owned privately where cost efficiency flies high above systematic security. This becomes more problematic when companies, public and private, are leaving open connections into these SCADA systems, just waiting for a hacker to do physical and/or monetary harm.

  The entire issue of cyber and SCADA security is impossible to encompass in one study so I have based my research mainly on the government's action, or perceived inaction, when it comes to the threat of a cyber attack. This issue cannot be all encompassing because of the statistics that I have just provided to you. However, I do believe that the government's response

to the issue and the academic community's belief in the threat is vital to the understanding of the complicated matter of SCADA security.

Using in-depth interviews from high ranking government officials and academics in the field of SCADA research and cyber security, I investigated the area of government involvement very thoroughly. With the use of thousands of pages of text and articles I have been able to gather a thoughtful representation of the true threat that our country faces with respect to the safety of our critical infrastructure. However, before I lay out my research some definitions, some definitions to this research must be given. I begin by defining terrorism and cyber terrorism.

Defining Terrorism

To begin a study on terrorism one must first identify its origins and unearth the reasons for its continued use. While the true origins of terrorism are unfeasible to identify many scientists pinpoint their beginnings with the sicarii, a terrorist movement that began in the first century. Walter Laqueur, a renowned terrorist expert, describes the sicarii as "a highly organized religious sect consisting of men of lower orders active in the Zealot struggle in Palestine" (Laqueur 3). While this organization did not bear the terrorist label at the time, its use of "unorthodox tactics such as attacking their enemies by daylight, preferably on holidays when crowds congregated in Jerusalem", are methods used by today's terrorists (Laqueur 3). Another highly influential terrorist organization was the Assassins, "an offshoot of the Ismailis who appeared in the eleventh century and were suppressed by the Mongols in the thirteenth" (Laqueur 4). This group is intriguing to many terrorism scholars because the tactics that were used are very comparable to the ones that are used by modern terrorists. In Laqueur's book entitled, The History of Terrorism, he stresses this relationship when he writes; "Their first urban victim was the chief minister of the Sultan of Baghdad […] a Sunnite by religious persuasion and therefore an enemy" (Laqueur 8). While these attacks may have been common throughout the Middle Ages and beyond, Laqueur outlines the lack of success these early groups experienced brilliantly when he writes,

> "Despite the considerable violence in Europe during the Middle Ages,
> and, even worse, during the religious wars of the sixteenth centuries, in
> which monarchs as well as religious leaders were killed, there were no
> sustained terrorist campaigns during this time" (Laqueur 5).

While these gruesome acts of terror were employed long before the 18th century it was not until the French Revolution were the word terrorism came about. It would become highly relevant from then on with the political and social disarray that came at the dawn of the 19th century. Bruce Hoffman, a terrorism expert, describes this era as "a time of great national tension and social ferment, witnessed the emergence of modern-what I call traditional-terrorism and guerrilla warfare" (Hoffman 5). In a time of inequality where political change was nearly impossible to produce from poor leftists, because of societal status, terrorism was seen as an effective way for a small highly motivated group to enact large political change.

By definition, terrorism at its foundation is the employment of terror as a mode of politics. Dan Verton, a journalist covering issues of terrorism and cyber security, writes, "Terrorism…is a form of politics that strikes fear in the hearts and minds of people because of its destructive power and its ability to wreak havoc and physical pain on unsuspecting innocent people" (Verton XIX). Martha Crenshaw, a terrorism scholar, also provides a brilliant example of the use of asymmetrical tactics used by terrorists when she writes, "Generally small organizations resort to violence to compensate for what they lack in numbers" (Crenshaw 11).

Terrorism is a strikingly useful tool for small groups to wage asymmetric warfare to further their influence on public policy. Essentially, many terrorists find it more useful to cause mass havoc in the matter of minutes, with sometimes less than ideal planning, than to sit down and negotiate diplomatically with the political opposition. However, as Crenshaw points out, terrorism is not always the first choice of action by these sub-national groups. Crenshaw writes, "In the Palestinian-Israeli struggle, terrorism followed the failure of Arab efforts at conventional warfare against Israel" (Crenshaw 11). Fundamentally, the reason that sub-national groups use terrorism is because they feel as though they can benefit from their terrorist activity, through free publicity and also frightened political leaders that they hope will become more committed to listen to their particular demands. However one may wonder why terrorists, who lack sufficient numbers, can become so dangerous and influential. This is due to their elusiveness and also their erratic nature. Crenshaw writes, "[…] the essential problem is when do extremist organizations find terrorism useful", and trying to determine the timeframe of this usefulness (Crenshaw 10). Terrorisms effectiveness also lays in its lack of borders. Hoffman writes, "Toward the end of the nineteenth century […] terrorist attacks took place in many places all over the globe" (Laqueur 12). Ultimately, no state can completely protect themselves from terrorist activity, however it can implement the proper policies that better prevent terrorism and also try and thwart the use of terrorism as a way for small under funded radical groups to gain political power and undermine the security of their nation.

Any political science scholar will tell you that terrorism is one of the most elusive terms to define in all of the social sciences. David Whittaker, a retired international relations lecturer, writes, "A troubled world, searching for consensus about the meaning of terrorism and how to counter it, finds it impossible to frame a workable definition" (Whittaker 11). Laqueur, describes terrorisms ambiguity best when he writes, "No definition of terrorism can possibly cover all the varieties of terrorism that have appeared throughout history" (Laqueur 17). "The word terrorism was first popularized during the French Revolution. "In contrast to its contemporary usage, at that time terrorism had a decidedly positive connotation" (Hoffman 15). While terrorism grew from very humble beginnings, at the turn of the 19th century it became used as a political tool to better the plight of the poor and under represented. "Ironically, perhaps, terrorism in its original context was closely associated with the ideals of virtue and democracy" (Hoffman 15). However, during the late 19th century a new definition of terrorism unfolded. Carlo Pisacane, an Italian revolutionary, outlined the use of terrorism as, "Violence […] necessary not only to draw attention to, or generate publicity for, a cause, but to inform, educate and ultimately rally behind the revolution" (Hoffman 17). This belief of terrorism as a revolutionary tool changed once again by the 1930s. "It was now used less to refer to revolutionary movements […] and more to describe practices of mass repression employed by totalitarian states and their doctoral leaders against their own citizens" (Hoffman 23). One of the most involved political terrorist movements of this time were the gangs that Mussolini and Hitler hired to harass and intimidate political opponents. While another shift took place after World War II, in the early 1980s with the rise of terrorism in the Middle East on western targets terrorism found a new meaning once again. Hoffman writes, "Terrorism thus became associated with a type of covert or surrogate warfare whereby weaker states could confront larger, more powerful rivals without the risk of retribution" (Hoffman 27). The definition of terrorism cannot be easily defined, even by the powerful bureaucracies of the United States. For example, different definitions exist in the department of state, FBI, and defense department in the United States. For the purpose of my

research I will use a rather exhaustive definition by Grant Wardlaw, a senior criminologist who writes,

> Political terrorism is the use, or threat of use, of violence by an individual
> or a group, whether acting for or in opposition to established authority,
> when such action is designed to create extreme anxiety and/or fear-
> inducing effects in a target group larger than the immediate victims with
> the purpose of coercing that group into acceding to the political demands
> of the perpetrators (Wardlaw 16).

While the definition of terrorism has continued to transform over the past two hundred years so have the tactics and tools of the terrorists. With the birth of the atomic bomb and the lethalness of new chemical and biological weapons it would be naive to believe that terrorists will not have their best opportunities to cause mass destruction and terror in the coming years. David Whittaker in his book, Terrorism Understanding the Global Threat, describes the imminent threat we face when he writes, "It is not impossible that a dirty bomb…could be assembled for use, perhaps, as a large car bomb" (Whittaker 174). While the implications of a massive coordinated attack have already been witnessed by the attacks of 9/11, it would be irresponsible to claim that terrorists are unable to strike again with this same brute force, even with our heightened security. Whittaker later states, "We all must now face the risk-picture where there is a possibility of such a highly organized, mammoth terror event occurring again" (Whittaker 161). If there is one thing that America has learned from the attacks on 9/11 it is that terrorists are not always unreliable, unskilled, madmen but in many cases are very clever and attune to the present day political landscape.

While physical threats continue to emerge the threat of a cyber-based attack grows more imminent. These attacks are presently occurring everyday with very little public knowledge and attention. Dan Verton writes, "There are tens of millions of people currently on the internet. If only a small fraction of these individuals have the necessary skills and training to launch destructive attacks this means […] thousands of individuals have such capabilities" (Verton IX). Verton goes on to state, "To date [2003], more than 50,000 computer viruses have been created, and up to 400 are active at any one time" (Verton IX). Not to complicate this issue further is the fact that while our physical infrastructure is aging we are relying more and more on SCADA systems that are linked to networks that can be exposed by skilled hackers and terrorists. While some assume that computer hackers are only interested in defacing government websites and stealing credit card numbers Maura Conway in her article, *What is Cyberterrorism?,* states, "in a briefing in late 2002, FBI assistant director Ronald Dick […] told reporters that hijackers had used the internet, and used it well" (Conway). This means that in early 2001 Al-Qaeda terrorists were already prepared to exploit the internet's vulnerabilities and use it to cause the most devastating terrorist attack ever committed on U.S. soil. Andrew Colarik, author of Cyber Terrorism, writes, "The loss of statewide power grids, the contamination or disruption of water grids, or the deliberate opening of a dams flood waters are but additional targets that have been penetrated in the past, and may in the future be employed by cyber terrorists to cause harm" (Colarik 52). In an interview with me he states, "Al-Qaeda and other low level terrorist organizations are prepared to exploit our cyber infrastructures vulnerabilities today" (Colarik).

Defining Infrastructure

If one is going to tackle the issue of infrastructure security they must first be prepared to give a rather precise definition to what exactly infrastructure is. For this I turn to The Merriam-Webster Dictionary which defines infrastructure as "a system of public works in a government, state or region" ("Infrastructure"). While this definition allows for a very broad characterization of infrastructure it still leaves much to be desired. A more thorough definition leads us to the 1996 Presidential Directive 131010 which defines infrastructure as,

> The framework of interdependent networks and systems comprising identifiable industries, institutions (including people and procedures), and distribution capabilities that provide a reliable flow of products and services essential to the defense and economic security of the United States, the smooth functioning of government at all levels, and society as a whole (Gheorghe 5).

While this definition is more thorough than the one found in Merriam-Webster yet it is still unable to truly define and outline all that the term infrastructure entails and represents. When I spoke with Andrew Colarik on the matter of defining infrastructure he told me that infrastructure was a broad term that must be all encompassing and is therefore in effect useless (Colarik). One may ask why it is so important to specifically define the word infrastructure and the answer is that for policies to be implemented properly to secure vital pieces of our country's public and private infrastructure one must be able to understand the true scope of all that the word infrastructure represents so that they may take the correct action may be taken. However, a vital road block to more thoroughly defining infrastructure lie with the ever changing physical and political environment that we live in. In a congressional research report released in 2004, commenting on the evolution of the term infrastructure, it stated, "Twenty years ago infrastructure was defined primarily with respect to the adequacy of the nation's public works. In the mid 1990's, however, the growing threat of international terrorism led policymakers to reconsider the word infrastructure in the terms of homeland security" (Motiff). This evolution of the term infrastructure with its inclusion of homeland security practices created a need for a definition of critical infrastructure. Over the past few years it has become more and more clear that we rarely deal in terms of infrastructure but rather deal in terms of critical infrastructure. However, this beefed up rhetoric has not made its way to producing actual results when in 2005 the American Society of Civil Engineers gave America's overall infrastructure a grade of D and proposed that it would take 1.6 trillion dollars over the next five years to get all sectors of infrastructure working in good condition ("2005 Report Card for America's Infrastructure")

> To define critical infrastructure I turn to the 2001 Patriot Act which states, systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters (Sensenbrenner).

In an interview with Dan Verton I asked him how he would define critical infrastructure and he replied, "Critical infrastructure is any piece of our infrastructure that could directly affect our nation's security and stability, therefore it is everything" (Verton). For the origins of the term critical infrastructure I turn to Ted G. Lewis, an expert on SCADA systems, who writes, "The term critical infrastructure did not exist before the 1990's. Then, from 1997 through 2003, the

definition of what constituted a critical infrastructure expanded from 8 to 13 sectors plus five key assets. Today it is difficult to identify sectors of the national economy that are not critical" (Lewis 29). One may ask why the term critical infrastructure has become so all encompassing. The answer to this is because we live in a society where all people are connected through a host of infrastructure whether it is a wireless cell phone grid, electrical power grid, water management services, internet use and so on. If one of these infrastructures were to be attacked there would be instability throughout a broad area rather than just localized effects. In a 2002 book by the Committee on Science and Technology for Countering Terrorism it states, "The openness and efficiency of our key infrastructures transportation, information and telecommunications systems, health systems, the electric power grid, emergency response units, food and water supplies, and others make them susceptible to terrorist attacks" (Albert's). This presumes that we are no longer a nation that can thwart off the effects of a localized attack on our nation's infrastructure because all the crucial components that make up critical infrastructure are susceptible and in effect networked.

Another division in the definition of infrastructure was the development of internet technologies and their expanded influence throughout the late 1980's through the present day. The 2003 National Strategy for Securing Cyberspace states, "By 2003, our economy and national security became fully dependent upon information technology and the information infrastructure. A network of networks directly supports the operation of all sectors of our economy…" (Cyberspace Threats and Vulnerabilities). The strategy further stated that the "healthy functioning of cyberspace is essential to our economy and national security" (Cyberspace Threats and Vulnerabilities). Even more terrifying, John Arquilla, a terrorism expert, told me during an interview that Al-Qaeda was gaining key victories in terms of cyber warfare such as engineers and experts in the field of information technology (Arquilla). In today's world Al-Qaeda can gain victories not only through terrifying suicide bombs and calculated terrorist attacks but also through inexpensive cyber warfare where costly and in some cases life threatening terror can be waged. When I spoke with Dan Verton on the issue of cyber terrorism and the effect it could pose to our economy and our infrastructure he referred to what we saw in 2001 with the week long shut down of Wall Street after 9/11 and the large ramifications that we saw in the business world because of the extended technological failures. He also told me that a prolonged shut down of Wall Street could pose a more than devastating effect on the U.S. economy than many suspect and could ultimately bring some sectors of our economy to their knees. The reason for this increasing insecurity and instability in the cyber world exists because "The U.S. has developed and implemented infrastructure that is more dependent on electronics, advanced telecommunications, energy supply systems…and transportation systems more than any other nation" (Maggio). Internet technologies (IT) are cost effective and are seen as a way to increase productivity and efficiency with little focus put on systematic security. Many terrorism experts believe cyber vulnerability "is the Achilles heel in which a good attack can disrupt everything that is connected in a massive scale" (Maggio). To make matters worse, 85% of our infrastructure is owned privately and there has been a lack of government-private party engagement in the field of cyber security, much of our infrastructure lay in the hands of CEO's who see no reward for their investment in security measures except for their own job security. Robert Graham, CEO of Errata Security, stated, "It's an industry in denial. They don't believe they have security problems that they have. It's not a technical issue, but a political one" (Higgins). This inaction cannot be blamed however on lack of knowledge of the threat. In a study by Trusted Network Technologies in 2006 50 IT CEO's from mid size electrical and gas

companies were asked about their cyber preparedness and their sense of the true threat that cyber terrorists pose. In a response to the statement asking about the future threat that online attackers pose to our critical electrical infrastructure, 40% of the respondents were neutral about the idea and 33% of the respondents either agreed or strongly agreed that systems could be compromised in the next 24 months (Walker). Knowledge of this is scary for many IT security personnel who believe that security is lacking to the extent that there are hundreds of open and firewall free networks waiting for terrorist sabotage that could cripple or severely damage vital pieces of our nation's critical infrastructure. In an alarming report by the Government Accountability Office (GAO) in 2007 it stated,

> With 85 percent of the country's critical infrastructure in private hands,
> the federal government must make sure that the 17 infrastructure sectors
> include cyber security in their plans to protect themselves against cyber
> attacks and disaster…However, none of the sectors included in their sector
> plans all 30 cyber security criteria, such as key vulnerabilities and
> measures to reduce them, the official also testified (Mosquera).

The harsh reality of the situation is that we will continue to invest and create new technologies that ever more bind the vital core of our infrastructure and soon create an infrastructure that is so interconnected the threat of terrorism no longer lays in a crowded city street but rather thousands of miles away through a key board and a mouse. As I was told in an interview with John Arquilla, "Distance is no longer a factor for terrorist across the world" (Arquilla).

Data and Methods

When I began my study on cyber terrorism and its impact on SCADA systems and infrastructure security I hypothesized that the threat posed by cyber terrorists was so grave that our nation was in critical danger. However, from my study I can conclude that while there is a great cyber threat there are also positive safeguards being put in place to hinder their clever and ever evolving opponents. However I can also conclude from my research that many sponsors of the government describe the problem as much less pressing than those involved in research and homeland security. I came to this conclusion with the use of in-person and telephone interviews, government testimony and other research tools.

The first portion of my data came from interviews with 10 government and private security specialists ranging from a government house representative, a senator, to data security specialists within the field of homeland security. These interviews spanned from September 15, 2007 through November 9, 2007 and each interview lasted approximately 15-50 minutes and was recorded with a mini-cassette recorder for future reference. To prepare for these interviews I researched the participant and then in a conversational manner discussed the issue of infrastructure security, vulnerability, and preparedness.

I also attended a security seminar, Operation Weblock, in Jacksonville, FL on October 18-19, 2007. Here representatives from the private and government sector spoke about the risks that are posed by cyber terrorists and how companies can better safeguard themselves from a devastating attack. It was at this seminar that I spoke with Dan Verton, a highly acclaimed investigative journalist and consultant for the government with cyber security affairs. I also met with cyber security experts from the Florida Department of Law Enforcement and learned of the policies that are being put in place to help secure Florida's online and physical infrastructure.

Lastly I consulted thousands of pages of text on a range of issues from cyber security, process control systems, SCADA systems, government effectiveness, and private company

responsibility. I used research databases provided by the University of North Florida and also gathered useful information from the local library system. I reviewed congressional testimony ranging from 2001 to 2007 on the issue of cyber security and infrastructure vulnerability. Dr. Ted G. Lewis, a researcher at the naval postgraduate school, also sent me helpful online links regarding the risk of cyber threats and the potential for a devastating attack on America's infrastructure and ultimately its citizens. From these sources I was able to create an exhaustive study of the issue of cyber terrorism and the serious threat it poses to our nation's infrastructure.

Results: The State of Our Infrastructure

With an ill prepared private sector and a government sector that is unwilling to truly regulate and stop the misuses and ignorance of powerful CEO's we are continuing down a path of inevitable failure. Through my research I have come to understand the misguided partnership that the government and the private sector have created over the past ten critical years. With most of the utility, wastewater management, and oil companies owned privately, cost effective business practices have led companies to implement systems such as SCADA into unsecured networks. Ultimately, the low cost of the internet has caused owners of critical infrastructure to implement patchwork security that could ultimately pose real threats to our economy and our citizen's lives.

> Until recently, SCADA systems were often used in a reactive manner to identify system faults as they occurred, recording system data and events for later analysis. With escalating demands on businesses for increased efficiency, SCADA systems have been re-architected to now include data management functionality that prevents problems, rather than recording them. Unfortunately, the security of SCADA systems is lacking, due to the narrow focus on using the systems for increased productivity, reliability and greater operating efficiencies ("SCADA: Get the Facts").

With much of our country becoming more and more technology driven a case can be made that security has taken a back seat to economic expansion. In an article by Security Focus it states,

> The electric power industry is perhaps the most obvious target, because the electric utilities are major users of sensor and control networks. Nearly 1,700 of the 3,200 power utilities have some sort of SCADA system in place, according to a recent survey by industry researcher Newton-Evans. Almost a quarter of companies with SCADA systems did not have a firewall separating the control network from the corporate network, leaving the systems open to attack from the Internet. In addition, only 40 percent of power utilities with such networks bothered to keep detailed access and network-data logs, according to Newton-Evans (Lemos).

In an article entitled, "The Threat of Electronic Warfare 2007", it stated, "It is the Achilles heal in which a good attack can disrupt everything that is connected in a massive scale" (Maggio). We see this same pattern when in an interview with John Arquilla I was told that because of the networking of our infrastructure critical nodes around the country are being created that could be damaged in the cyber or physical realm. In one article Robert Graham, CEO of Errata Security, stated, "It's an industry in denial. They don't believe they have the security problems they have. It's not a technical issue, but a political issue…Until there's a Pearl Harbor; there is no risk as far

as they are concerned" (Higgins). This is very telling because in an interview with Dan Verton he confirmed the belief that until there is a cyber Pearl Harbor the government will do little in the way of regulation. In 2003 Sandia National Laboratories released a report on SCADA security and concluded that, "The present state of security for SCADA is not commensurate with the threat or potential consequence" (Stamp). In an interview with Ted G. Lewis stated, the "problem is extensive and it would be hard for anyone to deny that" (Lewis). As you can see the threat that we face is very ominous and if not taken seriously and dealt with carefully and efficiently we as the most powerful country in the world could be brought to our knees with a metaphorical click of the mouse.

While much of this criticism applies to the private sector the government is in no position to preach about security. In an interview with Senator Bill Nelson he stated, "We are not moving in the right direction when it comes to cyber security and critical infrastructure protection" (Nelson). In another interview with Representative John Mica he stated, "The government must do more to create interaction within the public-private sectors" (Mica). However like in most grave instances where action is decisively needed many still profess that we are more secure than security officials are willing to claim because there has not been an attack that truly caused physical harm to civilians. While lives have yet to be lost one can pinpoint many instances that cyber attacks have taken place with financial costs reaching unimaginable heights and also reasonable scenarios that would appear to have the capacity to cause the loss of life. In a report about cyber attacks in 2003 top SCADA and cyber security officials concluded that the lack of data on cyber attacks is the reason for some of the industries complaints. In a 2002 article entitled *Debunking the Threat to Water Utilities*, it stated, "Most public utilities rely on a highly customized SCADA system. No two are the same, so hacking requires specific knowledge" (Byres). The problem with this logic is it lacks the research to truly reach its conclusion. If one were going to examine the industry of water utilities they would find that much of the substations that comprise the system are imported and the software that the system is run on is imported as well. This would negate the argument that specific knowledge would be needed to harness an attack because that knowledge lay with those outside the company and outside the country. In an interview with SCADA security expert Eric Byres he stated that the importation of critical and sensitive systems pose a real and dangerous threat. Also it is well known that SCADA software is in clear text on the internet and someone with a background in engineering coupled with computer software skills could cause a wide range of problems for any security system. Also more damning to this argument is the fact that while in 2000 the FBI reported that 71% of security breaches were carried out by insiders, or disgruntled employees who were familiar with the systems, that number has begun to dramatically change and in 2003 it was reported that 90% of security breaches originate outside the company (Byres). This leads one to believe that systems are either becoming friendlier to users that are unaware of company protocols or cyber terrorists are becoming more rampant and more skilled. "Regardless of the reasons, the threat sources are moving from internal to external and this needs to be taken into consideration in the risk assessment process" (Byres).

While the government has been very active over the last ten years when it comes to protecting critical infrastructure it is unclear as to how successful their attempts have been. In 1998 President Clinton signed PDD 63 which identified the various critical infrastructures and the need to protect them. What then followed were measures such as the 2001 Patriot Act and the 2003 Plan to Secure Cyber Space. While these measures coupled with increased congressional testimony have stirred up Washington and layed the foundation for the understanding of the

critical problem we face it is very clear that little improvement has been made. The most recent set of government guidelines came from the National Electrical Reliability Corporation (NERC). These guidelines include specific steps that companies must take to better secure their systems from a cyber attack. In an interview with Stan Johnson, spokesperson for NERC, I was told that the standards would be tough and while implementation would raise costs for electrical companies the guidelines were achievable and could prove to be very effective (Johnson). With these 83 guidelines coupled with the regulations under the Sarabaes-Oxlety Act (SOX) the need for increased cost effective practices may come to wreck more havoc on security (Walker). In an article by Trusted Network Technologies it stated, "Compliance also diminishes resources and diverts them form other important projects" (Walker). These policies however are ultimately a step in the right direction because they are enforceable and display that the government has the courage to take on electrical companies if it is what's needed to secure that vital core of our critical infrastructure. Later in my interview with Stan Johnson he stated, "We are going to implement policies that will require increased costs on security measures by companies and that is ok" (Johnson).

While government standards are a step in the right direction many experts have called on all industries, including the government, to map out a plan that would allow for assistance and response in the event of an attack. In a report by News Report it stated,

Our nation's Internet and cyber infrastructure serve as a critical backbone for the exchange of information vital to our security and our economy, but our analysis has exposed a significant weakness that could paralyze the economy following a disaster… If there's a cyber disaster, there is no emergency number to call -- and no one in place to respond because our nation simply doesn't have the kind of coordinated plan in place that we need to restart and restore the Internet," Rust added. "Government and industry must work together to beef up our cyber-security and recovery efforts" ("Analysis Warns U.S. of Cyber Security Weaknesses").

This is a very telling argument because it calls into question why our government seems to be so focused on emergency preparedness, as was outlined in the National Infrastructure Protection Plan, and yet little of the National Cyber Security Divisions budget is set for cyber recovery. Yet this question also leads us to the inquiry of government funding. In an article by the National Journal's Technology Daily in 2007, it stated that the budget for the department's cyber division was close to the same as the previous year and this was unacceptable. It further stated, "It is certainly a good sign that the president has requested $65.5 billion in IT spending across federal agencies agencies…But when you look at a breakdown of the percentages, specifically for [Homeland Security], the 1.1 percent decrease from last year is very concerning" (Greenfield). This issue also arose when I spoke with Sam Varnado, of Sandia National Laboratories, and was told that many of the agencies that are commissioned for cyber security are under funded and are lacking many necessary resources. He later when on to state, "If we are going to give true focus to the implementation of correct SCADA security measures programs must be funded that can create the necessary technologies" (Varnado). This is very concerning when one considers that as technology progresses the problem of cyber vulnerability within critical infrastructure will just become more and more dynamic and imposing. Again while many advances are being made within the government spectrum the change is not happening at a rate that could cause anyone to believe that we are headed for a more secure infrastructure. One key to securing our critical

infrastructure and our SCADA systems are providing effective policies for companies to follow that will provide for higher security. However as Eric Byres told me in my interview, "The government beurocrats continue to put out specific point plans that are neither possible to implement and knowingly not cost effective" (Byres). This would lead one to believe that the government is interested in a strategy that is not so much concerned about security but rather a plan that does not leave the government as the fall guy. To finally display the threat that cyber terrorists pose to our critical infrastructure I turn to an article by Trusted Technologies, which spoke with 50 IT executives of Utility companies around the country, came to the conclusion that "Utilities clearly recognizes the threat—and don't just consider but expect an outside attack on critical SCADA and energy distribution systems" (Higgins). This alarming conclusion comes from the discovery that "one third of IT executives surveyed believed that some SCADA or distributions systems would be attacked or compromised in the next two years" (Higgins). In the end my results concur with beliefs of Dan Verton who relayed to me in my interview that the government cannot be relied on to secure our cyber infrastructure but yet we must turn to partnerships of private business executives, IT experts and government officials for one to even scratch the surface.

Implications and Conclusion

From my interviews with government officials and security personnel I can conclude that the government since early 2002 has been studying the threats that the cyber world has on our critical infrastructure very heavily. This can be seen from the increase in congressional reports and increased congressional testimony being given by the leaders in cyber security on Capitol Hill. However, with over 85% of our infrastructure being owned privately and many turning to the internet for increased efficiency and lower costs it seems as though we are at critical point in the world of cyber security where the entire infrastructure could soon be so robust there would be no turning back the years of lacking security protocols. When I spoke with John Arquilla on the subject of government action he stated that while there has been much progress made in Washington "they cannot be relied on to secure the systems of the entire nation" (Arquilla). Sam Varnado presented to me that a major problem associated with government is funding for institutional research in the field of cyber security. With respect to the IT Homeland Security budget for the 2008 fiscal year "the Bush budget proposal requests 179 million for department-wide IT expenses. That would be down 90 million from the 2007 budget" (Greenfield). This report prompted Liesyl Franz, a budget analyst, to respond, "With it's mission and increased expectations that is insufficient" (Greenfield). While the government may be spending billions of dollars to prevent a serious cyber attack one could present evidence that shows that the plutocracy that the government has created has led to a place where a cyber emergency bureaucracy has no 911 number to call for help. Edward Rust proclaims "If there's a cyber disaster, there is no emergency number to call—and no one in place to respond because our nation simply doesn't have that kind of coordinated plan in place…" ("Business Roundtable Issues Warning"). An example of this would be the National Cyber Security Division's funding is targeted for support of cyber recovery. From my research I have found that there is a true consensus around the entire business and government community that the threat of cyber attack is real and will only progressively become more problematic as the country moves more critical systems to the vulnerable internet. In the end one can turn to the Journal of Counterterrorism and Homeland Security for the answer on our cyber preparedness when they state, "The U.S. has developed and implemented infrastructure that is more dependent on electronics, advanced

telecommunications, energy supply systems, information/computer networks, and transportation systems more than other foreign nations" (Maggio).

My results indicate that the threat of a cyber attack on the critical infrastructure of the United States is a real and ongoing threat. My three main findings conclude that the United States government, while aware of the threat, is not acting accordingly. The emergency preparedness programs that the government has set up for are not sufficient enough to combat a cyber attack, and also the highest of executives in the energy, academic, and security sectors believe that the threat of a cyber or physical attack on our critical infrastructure is not only real but imminent. From my research I have collected sufficient evidence to conclude that the infrastructure of the United States is progressing in a manner that will continually combat the forces of regulation and leave much of our most critical infrastructure vulnerable to either a physical or a cyber attack that could result in billions of dollars in losses as well as the loss of lives. When I spoke with Dan Verton about the state of our infrastructure protection he stated, "Companies are waiting for the electronic Pearl Harbor or a cyber attack comparable to hurricane Katrina before they truly enact policies that promote real security and secure their systems" (Verton).

While my research outlined the inaction of the government and the overall threat that of a cyber attack on our critical infrastructure more needs to be done to truly combat the problem. Laboratories that are funded by the Department of Defense and Department of Energy are constantly producing terrifying reports about the state of our SCADA system security and also the vulnerabilities of our physical infrastructure to cyber attack. However many of these reports findings do not make their way into company security audits. I believe that Capital Hill is taking the correct action by giving the floor to cyber experts so that action can be taken for the most desperate of needs. One of the major steps that need to be taken is to outline the beurocracy of the cyber security community more thoroughly and outline the duties of the different departments so that information sharing can take place in the most efficient manner. With the United States becoming more dependent on insecure technologies and the reality that powerful CEO's are unwilling to sacrifice cost efficiency for security, the problem of cyber security will become more jumbled and will soon, if no action is taken, become too much for an interconnected system of unsecured parts to truly overhaul, and protect.

References

Albert's, Bruce, and William A. Wulf. Making the Nation Safer: the Role of Science and
    Technology in Countering. New York: National Academies, 2002.

"Analysis Warns U.S. of Cyber Security Weaknesses." Government Technology. 27 July
    2006. News Report. 21 Nov. 2007 <http://www.govtech.com/gt/articles/100012>.

Arquilla, John. Telephone interview. 14 Nov. 2007.

"Business Roundtable Issues Warning on Lack of Preparation to Recover the Internet
    Following a Catastrophic Cyber Disruption." Business Roundtable. 23 June 2006. 12
    Nov. 2007 <http://www.businessroundtable.org/newsroom/document.aspx>.

Byres, Eric, and Justin Lowe. The Myths and Facts behind Cyber Security Risks for
    Industrial Control Systems. British Columbia Institute of Technology. Burnaby, 2003. 15
    Nov. 2007.

Byres, Eric. Telephone interview. 15 Nov. 2007.

Colarik, Andrew. Telephone Interview. 22 Sept. 2007.

Colarik, Andrew. Cyber Terrorism: Economic and Political Implications. New York: Idea
        Group Incorporated, 2006.

Conway, Maura. Reality Bytes: Cyberterrorism and Terrorist 'Use' of the Internet. First
        Monday. 2002. 19 Nov. 2007
        <http://firstmonday.org/issues/issue7_11/conway/index.html>.

Crenshaw, Martha. Terrorism in Context. New York: Pennsylvania State UP, 1994.

Cyberspace Threats and Vulnerabilities. White House. 2003. 22 Oct. 2007
        <http://www.whitehouse.gov/pcipb/case_for_action.pdf>.

Gheorghe, Adrian V. Critical Infrastructures at Risk: Securing the European Electric
        Power. Springer, 2006.

Greenfield, Heather. "Bush's Cybersecurity Budget Proposal Concerns Tech Industry."
        National Journals Technology Daily (2007).

Higgins, Kelly. "SCADA State of Denial." Insecure.Org. 16 Apr. 2007. 10 Oct. 2007
        <http://seclists.org/isn/2007/Apr/0068.html>.

Hoffman, Bruce. Inside Terrorism. New York: Columbia UP, 1998.

"Infrastructure." Mariam-Webster Online. Mariam-Webster. 11 Oct. 2007
        <http://www.m-w.com/dictionary/infrastructure>.

"Internet Usage Statistics." Internet World Stats. Nov. 2007. Miniwatts Marketing Group.
        15 Oct. 2007 <http://www.internetworldstats.com/stats.htm>.

Johnson, Stan. Telephone interview. 11 Nov. 2007.

Laqueur, Walter. A History of Terrorism. New York: Transaction, 2001.

Lemos, Robert. "U.S. Makes Securing SCADA Systems a Priority." 25 Oct. 2005.
        Security Focus. 22 Oct. 2007 <http://www.securityfocus.com/news/11351>.

Lewis, Ted G. Telephone interview. 8 Oct. 2007.

Lewis, Ted G. Critical Infrastructure Protection in Homeland Security. New Jersey:
        Wiley-Interscience, 2006. 229.

Maggio, Edward, and Kevin Coleman. "The Threat of Electronic Warfare 2007." Journal
        of Cyberterrorism and Homeland Security International 13 (2007): 1.

Mica, John. Telephone Interview. 10 Sept. 2007.

Mosquera, Mary. GAO: Infrastructure Plans Lack Cybersecurity Strategy. Federal
        Computer Week. Government Accountability Office, 2007. 12 Nov. 2007
        <http://www.fcw.com/online/news/150679-1.html>.

Motiff, John, and Paul Parfomak. Critical Infrastructure and Key Assets:. CRS Report for
        Congress. The Library of Congress, 2004. 26 Nov. 2007
        <http://www.fas.org/sgp/crs/RL32631.pdf>.

Nelson, Bill. Personal Interview. 19 Oct. 2007.

"SCADA: Get the Facts." Cyber Security Industry Alliance. 2008 Cyber Security
        Industry Alliance (CSIA). 13 Nov. 2007 <http://www.csialliance.org/issues/scada/>.

Sensenbrenner, James. United States. Cong. The USA Patriot Act. 107 Cong. H.R.3162.
        23 Oct. 2001. 24 Oct. 2007 <http://thomas.loc.gov/cgi-bin/bdquery/z?d107:h.r.03162:>.

Varnado, Sam. Telephone Interview. 17 Oct. 2007.

Verton, Dan. Black Ice: the Invisible Threat of Cyber-Terrorism. New York: McGraw
        -Hill, 2003.

Verton, Dan. Personal interview. 7 Sept. 2007.

Verton, Dan. "Terror.Com." Florida Department of Law Enforcement. Operation
        Weblock. Ponte Vedra Convention Center Marriot, Jacksonville, FL. 7 Sept. 2007.

Walker, Doug. "Utility IT Executives Expect Breach of Critical SCADA Systems."
        Pipeline and Gas Journal (2006): 1-3.

Weblock. Ponte Vedra Convention Center Marriot, Jacksonville, FL. 7 Sept. 2007.

Wardlaw, Grant. Political Terrorism: Theory, Tactics and Counter-Measures. New York:
        Cambridge UP, 1989.

Whittaker, David. Terrorists and Terrorism in the Contemporary World. New York:
        Routledge, 2004.

"2005 Report Card for America's Infrastructure." Report Card for America's
        Infrastructure. 2005. American Society of Engineers. 9 Nov. 2007
        <http://www.asce.org/reportcard/2005/index2005.cfm>.