Critical Infrastructure and Cyber Security

A project by Dr. Engel's Capstone at the Bush School of Government and Public Service

Created for CENTRA Technology – 5/6/2011

TEAM MEMBERS

Abby Doll, Renee Pirrong, Matthew Jennings, George Stasny, Andy Giblin, Steph Shaffer, and Aimee Anderson

Table of Contents

Introduction

Executive Summary

We were tasked by CENTRA Technology, Inc. to create a methodology that could be used to prioritize critical cyber assets in the United States. We have answered that call by developing a user-friendly, consequence-based methodology that requires the end user to carefully consider their cyber assets' contributions to vital missions of national security, economic security, and public safety. The user will be able to clearly visualize the potential impact of a loss of cyber assets on those three indicators vis-à-vis one another, which is especially important in the midst of the current budgetary uncertainty in Washington. In this study, we first present our definitions of the three indicators, an overview of the 18 sectors of critical infrastructure and commonalities and characteristics of their operating systems, a brief review of the literature on cyber security to date, and, of course a thorough discussion of the intricacies of how our methodology works.

Outline of the Problem

Over the past few years, computers and the Internet have become an omnipresent force within the American economy. Industries considered to be vital to the nation's well being rely increasingly technology to improve their day-to-day functions. Greater dependency on cyber assets has also opened up many industries to numerous vulnerabilities that can be manipulated through accidental or malicious intent. The Federal Government has acknowledged the problem of cyber-attacks that could arise because of these vulnerabilities in the system. Though all agree on the existence of these problems, consensus on how to most effectively address them has proven to be much more difficult.

The problem of prioritizing infrastructure begins at the definition of infrastructure. The Congressional Budget Office made the first attempt to define infrastructure in 1983 saying that infrastructure was the common characteristics of levels of government that were directly critical to the nation's economy. The report cited highways, public transit systems, wastewater treatment works, water resources, air traffic control, airports, and municipal water supply as examples of infrastructure[1]. This vague definition obviously could not be used as a working definition because it does not inform the reader on what the characteristics are, what is critical, or what would constitute a common attribute. This definition was quickly replaced by another broader definition in 1984, and in the subsequent decade the term infrastructure operated under one vague definition after another. In 1998 the President's Commission on Critical Infrastructure produced a slightly different definition of "those physical and cyber-based systems essential to the minimum operations of the economy and government[2]. This was the first time the government had used the term critical in a working definition as a way to begin prioritizing the demands from the country's infrastructure on the government.

[1]Moteff, John, and Paul Parfomak. United States. *Critical Infrastructure and Key Assets: Definition and Identification*. , 2004.
[2]Moteff, John, and Paul Parfomak.

On October 4, 2001, the Senate held a hearing to determine the direction of the country's cyber security. They designated responsibility for cyber-security to the newly formed Department of Homeland Security, a duty that has continued to today[3]. The group was tasked with creating a method of protecting the critical components of the country's infrastructure from cyber attacks. The DHS originally listed 12 sectors as "critical" under this plan, but the list has expanded to the current count of 18.[4]

The DHS's approach addresses all of the sectors equally. They produce a National Infrastructure Protection Plan (NIPP) every year, which prioritizes infrastructure and explains the characteristics and functions of each sector. The problem with this system is that because all sectors are valued to be equally important, policy makers cannot accurately assess criticality. While all infrastructures may contribute to American economics, politics, or culture, some are more important for the nation to function. Furthermore, since each sector relies on cyber assets with varying degrees, protecting some cyber assets may be more important in one sector than another. The government has communicated their desire for a more comprehensive approach to prioritizing, though it hasn't been successful yet. In President Bush's *National Strategy for Physical Protection of Critical Infrastructure and Key Assets*, the administration suggests that a master list of assets to determine prioritization, and yet then acknowledges that a ranking of individual assets could be very fluid. The report goes on to call for a uniform methodology for DHS to identify individual assets that could be considered critical. However the subsequent attempts proved to be ineffective because of some inappropriate assets that appeared on their results.[5]

Since 1984 the concept of infrastructure has expanded beyond the government's original vague definition. Officials have added to the list of "critical assets" rather than limiting the list to what is truly important and necessary in the current economic and security climate. By creating a more objective and comprehensive prioritization system, the DHS and others tasked with deciding how to best protect numerous types of infrastructure may be able to better allocate their scarce funds.

Definitions of Key Terms

Since there are a lot of terms in the literature and in the field, we felt it was necessary to ensure a common understanding for the purposes of this project. Therefore, we offer the following definitions and key terms to be used throughout the project. As this study is focusing on critical infrastructures through the lens of the Department of Homeland Security (DHS), the definition for "critical infrastructure" is borrowed from their National Infrastructure Protection Plan (NIPP).

---

[3]United States. *Critical Infrastructure Protection: Who's in Charge?* Washington D.C.: U.S. Government Printing Office, 2002. Print.

[4]"Sector-Specific Plans." *National Infrastructure Protection Plan: Critical Manufacturing Sector*. Department of Homeland Security, 18 Apr 2011. Web. 21 Apr 2011. <http://www.dhs.gov/files/programs/gc_1179866197607.shtm>.

[5]Moteff, John, and Paul Parfomak.

Critical Infrastructure and Key Resources: Systems and assets, whether physical or virtual, so and vital that the incapacity or destruction of such may have a debilitating impact on national security, national economic security, public health or safety, environment, or any combination of these matters, across any Federal, State, regional, territorial, or local jurisdiction.[6]

One notices, however, that "criticality" or the prioritization elements listed in the above definition ("national security, national economic security, public health or safety, environment, or any combination of these matters") are never clearly defined. Therefore, in order to begin a process to measure criticality and prioritize infrastructures in terms of their importance in national security, economic security, and public safety, we must create definitions for these three elements to enable their use as tools in measuring criticality.

Figure 1

Surveying the literature, it becomes clear that the elements of national security, economic security, and public safety are fluid and, in essence, bleed between each other in terms of their missions and components (See Figure 1). For example, President Obama's National Security Strategy encompasses not only military and governance elements but also elements of economic prosperity and national development capacity.[7]

Though in other contexts the definitions for the three elements may intersect, for this study we have attempted to separate the definitions of national security, economic security, and public safety from one another, to the extent possible.

National security: The protection, maintenance, and resilience of the federal government's ability to conduct military operations; implement effective law enforcement; collect, analyze, and disseminate all-source intelligence in a timely fashion; conduct foreign affairs; and ensure effective governance.

Military capability

Military capability refers to the ability of the U.S. military to conduct basic operations. This includes, but is not limited to, deploying troops and supplies abroad to secure vital interests, conducting bombing missions to achieve air superiority in a conventional conflict, conducting humanitarian missions and escort operations on the high seas, interdicting dangerous cargo before it enters the United States, and carrying out special operations where necessary.

[6] "National Infrastructure Protection Plan." Department of Homeland Security, 2009: 109.
[7] "National Security Strategy." The White House, May 2010. Retrieved 20 Apr 2011. http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf

Law enforcement capability

Federal law enforcement capability refers to the ability to maintain the rule of law, through the federal court system. While the Department of Justice's investigative capabilities are important, they are predominantly associated with corporate cases and white-collar crimes. Thus, our references to federal law enforcement will refer to a functioning federal judiciary with the authority to pass legally binding judgment on cases brought before it.

Intelligence collection capabilities

The capability to gather intelligence refers to the ability of the 17 U.S. intelligence agencies to collect information from domestic and foreign sources. This includes the ability to securely deploy assets and collect, transmit, process, analyze, and disseminate signals intelligence (SIGINT), communications intelligence (COMINT), electronic intelligence (ELINT), human intelligence (HUMINT), imagery intelligence (IMINT), and measurement and signatures intelligence (MASINT). This also refers to the ability to collect these forms of intelligence against state actors, non-state actors, and individuals of interest to the U.S. federal government. This also includes the ability to share and receive such intelligence from intelligence sharing agreements with the NATO and "five eyes" community.

Foreign affairs

The ability to conduct foreign affairs refers to the ability of the federal government to establish, operate, and secure, diplomatic missions around the world. This includes the ability to deploy, secure, and communicate with ambassadors to dispatch policy direction and receive diplomatic cables. It includes the ability to communicate with U.S. allies on important policy matters and securely transport and communicate with the President of the United States, as chief diplomat, around the world as necessary to conduct negotiations with foreign counterparts.

Effective governance

The ability to effectively govern refers to the ability to continue the democratic system of government. This includes having popularly elected executive and legislative branches and an independent judiciary capable of incorporating the will of the people into policy decisions at the federal level. This includes the ability of the federal government to provide an acceptable degree of transparency in the policymaking process and the ability of the people to provide feedback to those policymakers.

Justifications for inclusion/exclusion

We feel that the five components above represent the most basic functions of federal government that protect its country from existential physical threats and provide policymakers with necessary information to make decisions on a daily basis.

Upon reading our definition of national security, the reader will note two important assumptions. First, our definition excludes "soft" security like economic and social issues. We understand that many would argue that the concept of national security encompasses much more

than the above-mentioned "hard" security issues. For instance, a vibrant network of private defense contractors allows for the financing of research and development (R&D) for military equipment, which is used to satisfy the function of military capabilities. Therefore, one can quite legitimately assert that economic security should also be included as an essential component of national security. Similar cases could be made for environmental security, food security, job security, and other factors. However, our approach is that such overlap, to an extent, hinders constructive dialogue when trying to examine each definition individually.

Second, our five components of national security, especially law enforcement and governance, are deliberately focused toward federal government functions. In turn, it excludes functions that pertain predominantly to the state, local, or tribal levels. For example, we have assessed that the ability of law enforcement entities to quickly response to incidents on a daily basis is not a matter of national security. It is, however, important in our subsequent definition of "public safety."

Our definition of "national security" was derived from the following definitions from government sources, scholars, and dictionaries:

- *President Obama's 2010 National Security Strategy* defines U.S. national security capacity as "the strength of our military, intelligence, diplomacy and development, and the security and resilience of our homeland."[8]

- In a 2010 joint publication, *the Joint Chiefs of Staff (JCS)* define national security as "A collective term encompassing both national defense and foreign relations of the United States. Specifically, the condition provided by: a. a military or defense advantage over any foreign nation or group of nations; b. a favorable foreign relations position; or c. a defense posture capable of successfully resisting hostile or destructive action from within or without, overt or covert."[9]

- Famous scholar and diplomat *George Kennan* once described national security as "the continued ability of this country to pursue its internal life without serious interference."[10]

Various dictionaries define national security as:

- "…a collective term for the defense and foreign relations of a country, protection of the interests of a country,"[11]

---

[8] United States. White House. Office of the President of the United States. *National Security Strategy*. By Barack H. Obama. May 2010. 14 Mar. 2011. http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf

[9] United States. Joint Chiefs of Staff (JCS). *Department of Defense Dictionary of Military and Associated Terms*. Defense Technical Information Center, 8 Nov. 2010. 15 Mar. 2011. http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf

[10] *Comments on the Economic and Security Implications Of Recent Developments in the World Oil Market*, 107th Cong. (2000) (testimony of Robert E. Ebel). http://hsgac.senate.gov/032400_ebel.htm

[11] "National Security | Define National Security at Dictionary.com." *Dictionary.com | Free Online Dictionary for English Definitions*. 27 Mar. 2011. http://dictionary.reference.com/browse/national+security

- "The foundation for the development of valid national objectives that define US goals or purposes. National security interests include preserving US political identity, framework, and institutions; fostering economic well-being; and bolstering international order supporting the vital interests of the United States and its allies,"[12] and

- "…the protection of nation from danger: the protection of a nation from attack or other danger by maintaining adequate armed forces and guarding state secrets."[13]

Economic security: Ensuring the security, flow and integrity of monetary and financial data and the control systems that manage the flow of goods and services through interstate and international trade.

Security of monetary and financial data

The security of monetary and financial data refers generally to the ability of businesses and financial institutions to keep data at an appropriate level of privacy. With the increasing interconnectedness of banking communications systems, there is a constant threat of unauthorized access to private information. This access does not require that an attacker have the ability to modify or disrupt any data, but merely to observe and copy it. Attacks of this sort are most generally used for improper authentication, or "identity theft," and can also be used for insider trading.

Flow of monetary and financial data

Flow refers simply to the continued successful operation of the monetary and financial system. Many attacks are designed to disrupt inter-firm and interbank transfers and communications, and while these attacks may not steal or alter wealth or sensitive information, they can slow down or even halt legitimate business operations. This is a critical component of our definition given that an economy ceases to operate as such without the ability to communicate and transfer wealth.

Integrity of monetary and financial data

Integrity refers wholly to the accuracy and authenticity of legitimate monetary information flowing through the economy. Any attack, which seeks to manipulate or fundamentally alter legitimate data, is regarded as an attack on data integrity. Most often this kind of attack is enabled by a breakdown in security, as the security flaw is generally used to gain the access required to conduct an attack on data integrity. In the digital age, this kind of attack is perhaps the most

[12] "National Security Interests - Definition of National Security Interests by the Free Online Dictionary, Thesaurus and Encyclopedia." *Dictionary, Encyclopedia and Thesaurus - The Free Dictionary*. 27 Mar. 2011. http://www.thefreedictionary.com/national security interests
[13] "National Security." *Encarta Dictionary*. Encarta Online, 2009. 27 Mar. 2011. http://encarta.msn.com/dictionary_1861696682/national_security.html

damaging given that it can be very difficult to recover data back to a true and valid state once an attack is carried out, often resulting in a direct loss of legitimate wealth.

Security of control systems that manage the flow of goods and services

The U.S. economy is a complex web of logistical, communication and transportation networks that manage and determine the flow of goods and services. Cyber assets support these networks and are critical for goods and services to move in the domestic and international markets. These control systems must function correctly in order for goods and services to flow from producers to consumers.

Justification for inclusion/exclusion

There are very few definitions of economic security. Most definitions pertain to the economic welfare and prosperity of a country or a stable income and standard of living over time. The Economic Security Index defines economic security as "the degree to which individuals are protected against hardship-causing economic losses." For the purposes of our project on cyber security, these definitions are insufficient for the following reasons:

First, we must examine the level of responsibility held by the government in protecting the economic wealth or "well-being" of the nation.[14] It is widely agreed that a major role of the United States government is to provide a fair and stable foundation from which a classically liberal open market can operate unencumbered. Basic protections such as prevention of fraud and theft, and the prosecution of those who violate these laws are absolutely essential to our economic system. The question, then, is to what extent does the concept of economic security include the notion of economic well-being, that is, the absolute per-capita value of wealth-generation by Americans?

Second, any measurement the impact of a cyber incident on the welfare of individuals will be intrinsically biased by value judgments made by the assessor. One would have to distinguish between first and second order effects of the incident, reconcile different types of loss to a single unit of measurement, and could never fully comprehend all consequences.

Any comprehensive risk analysis requires metrics on the level of impact. When assessing impact on economic security, certain factors such as the ability of economic agents to conduct trade and investment, transact goods, services and financial assets, and communicate securely are indisputably important. However, we find metrics that seek to aggregate overall wealth or well-being run the risk of committing government resources to the promotion of individual economic actors rather than toward the system as a whole. Furthermore, if the government can successfully provide a secure economic environment with a stable flow of goods and services and maintain the integrity of the system as a whole, legitimate wealth will inherently be protected. It is for this reason that we choose to limit the scope of our definition of economic security to pertain only to

[14] For other definitions, see Jones, Barry (2001). "Economic Security". Routledge Encyclopedia of International Political Economy: Entries P-Z. Pp 1377 and the "ILO Socio-economic Security Program". http://www.ilo.org/public/english/protection/ses/download/docs/definition.pdf. Both definitions pertain to the nation's or individual's economic well-being.

the function and robustness of the economy rather than the perceived aggregate economic well-being of individual economic agents, as other definitions might.

Public Safety: The preservation, maintenance, and resiliency of a state/local government's ability to mitigate disease outbreak, ensure timely response of emergency services, ensure an effective law enforcement presence, and provide access to basic needs for its area of jurisdiction.

Disease Outbreak Mitigation

According to the World Health Organization (WHO), a disease outbreak is the occurrence of cases of disease in excess of what would normally be expected in a defined community, geographical area or season[15]. Therefore, the mitigation of a disease outbreak is the ability to prevent the spread of virus or bacterial agent throughout a concentrated region.

Timely response of emergency services

The three main emergency services functions are police, fire and rescue services, and emergency medical services. These organizations must be able to communicate both with the community and each other in order to respond in a timely manner. For this project, a timely manner refers to an amount of time that is not in an excess of time greater than the normal response time as to lead to additional deaths or injuries, solely attributable to a lack of response.

State and local law enforcement presence and response

Presence and response of state and local law enforcement refers to the ability of these agencies to communicate both with the community and each other in a timely manner and respond appropriately and effectively. These agencies include county sheriff's departments, city police departments, university police departments, transit authority agencies, and other miscellaneous law enforcement entities.

Access to basic needs

This refers to the ability of the state and local governments in a state of emergency to provide for its area jurisdiction five basic survival needs: air, water, food, clothing, and shelter. This includes:

- Access to open and functioning grocery stores,
- Clean, running water,
- Clean, breathable air,
- Sound structures for shelter, and
- Adequate clothing for protection against the elements

[15] "Disease Outbreaks." World Health Organization (2011). <http://www.who.int/topics/disease_outbreaks/en/>.

To define public safety, research was done to determine previous definition of public safety and how they related to this project. However, very few definitions beyond general statement could be found that could be applied to this project. For example, one example was from the Suburban Emergency Management Project that defined public safety as:

> The prevention of and the protection of the general population from, all manners of significant danger, injury, damage, or harm. This prevention and protection traditionally is provided by police, fire, emergency medical services, and communications.[16]

However, this definition was not found suitable as it did not delve into the different functions of public safety, which were necessary for this project. Therefore, our group expanded the general definitions of public safety to include functions and components as required by our study.

Cyber Assets and Cyber Incidents

For the scope of this study, we felt it was also necessary to define the terms of "cyber assets" and what constitutes a "cyber incident."

Cyber Assets: Programmable electronic devices and communication networks including hardware, software, and data.[17]

Cyber Incident: The act of violating an explicit or implied security policy. These include but are not limited to:

- attempts (either failed or successful) to gain unauthorized access to a system or its data
- unwanted disruption or denial of service
- the unauthorized use of a system for the processing or storage of data
- changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent.[18]

[16] "Disaster Dictionary." Suburban Emergency Management Project (2007): n. pag. Web. 4 May 2011. <http://www.semp.us/publications/disaster_dictionary.php?letter=P>.
[17] "Incident Definition." US-CERT. U.S. Department of Homeland Security, Retrieved 28 Jan 2011. http://www.us-cert.gov/federal/incidentDefinition.html,
[18] Ibid.

Critical Infrastructure Sectors: Overview

We determined it necessary to complete a brief review of the 18 sectors of critical infrastructure, as outlined by the Department of Homeland Security (DHS). These summaries are not meant to be comprehensive. Rather, they are intended to provide the end user of our methodology with basic knowledge about the cyber assets and functions, geographic distribution of the sectors, and broad trends of how cyber assets in each sector may be used in the future.

Agriculture and Food Sector

The Agriculture and Food sector provides sustenance for millions of people throughout the nation and across the world. It is segmented into approximately 2.1 million privately owned farms, 850,000 firms and over one million firms.[19]

Cyber Assets and Functions

According to the Department of Homeland Security's sector-specific plan, the Agriculture and Food sector is not a target for cyber-attack.[20] This is due to three primary reasons. First, the sector is unlikely to be an attractive financial target because a cyber attack would yield little monetary gain. Second, the Agriculture and Food sector is fragmented into different companies which are responsible for different stages of production. So, a cyber attack on any one company or production stage would not have a substantial impact downstream. Third, there are a variety of different countermeasures already in place at the federal level that provide some protection from attack. This includes the Federal Information Security Management Act (FISMA) that requires agencies to adequately secure their information systems and to designate an information security officer.

Geography

The Agriculture and Food sector is geographically disbursed throughout the nation without a single focal point. Different geographic regions may have crops or produce that is more prevalent or specific to that area, but it is dispersed throughout the U.S.

Future Trends

There are no major trends in the Agriculture and Food sector in regards to cyber assets or cyber security.

Banking and Finance

[19] United States. National Infrastructure Protection Plan: Agriculture and Food Sector. , 2008. 17 Apr 2011. http://www.dhs.gov/xlibrary/assets/nipp_snapshot_agriculture.pdf

[20] United States. Food and Agriculture Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan. , 2010. 17 Apr 2011. http://www.foodshield.org/docs/2010%20Food%20and%20Agriculture%20Sector%20Specific%20Plan%5B1%5D.pdf

The financial industry is highly regulated by private and public entities at the state and national level. The system of regulatory agencies is extremely complex, particularly regarding their relationships and jurisdictions. According to DHS, the Banking and Finance sector is made up of the following institutions:[21]

- Depository financial institutions (banks, thrifts, and credit unions)
- Insurers
- Securities brokers/dealers
- Investment companies
- Certain financial utilities

Cyber Assets and Functions[22]

The four main functions facilitated by these institutions and their products are:

- Allow customers to deposit funds and make payments to other parties;
- Provide credit and liquidity to customers;
- Allow customers to invest funds for both the long and short term, and
- Transfer financial risks between customers.

The two largest cyber assets employed by retail banks are Systems, Applications, and Products in Data Processing (SAP) and PeopleSoft, with SAP being the larger of the two.[23] In fact, SAP is the market leader in enterprise application software. The SAP for Banking software package essentially provides all the applications a financial institution needs to perform its daily business activities, including loan management, checking and deposit account operations, collateral management, lease operations, integrated accounting, risk and compliance management, enterprise performance management, customer relationship management, and price optimization.[24] PeopleSoft is a package of enterprise applications produced by Oracle that is a competitor of SAP and essentially performs the same functions.[25]

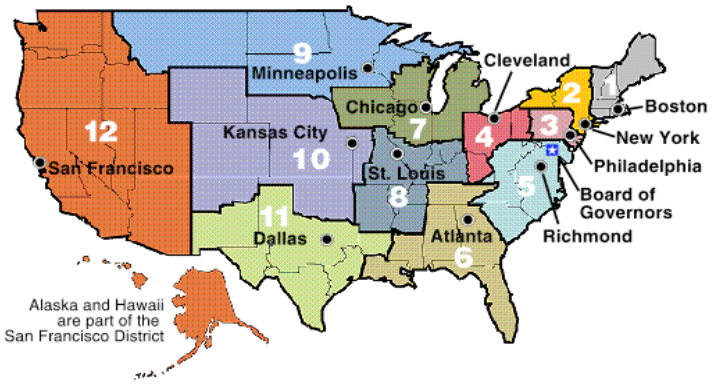
At the federal level, the most critical cyber asset of the Federal Reserve Bank is a system called Fedwire, which is used to transfer and process payments between the Federal Reserve and local banks. The Automated Clearing House (ACH) and Clearing House Inter-bank Payment System (CHIPS) are also necessary for the Federal Reserve to perform daily functions.[26]
The Banking and Finance sector has largely modernized at the same pace as technology. In turn, the sector is highly reliant on computers and cyber assets. Before the widespread dependence on cyber assets, the largest available printed bank note was a $100,000 bill. However, because larger transactions are now conducted electronically, the largest available bank note is $100.

---

[21] Banking and Finance Sector: Critical Infrastructure and Key Resources. 29 December 2008. Department of Homeland Security. 28 February 2011. http://www.dhs.gov/files/programs/gc_1188566544964.shtm
[22] Banking and Finance Sector: Critical Infrastructure and Key Resources. 29 December 2008. Department of Homeland Security. 28 February 2011. http://www.dhs.gov/files/programs/gc_1188566544964.shtm
[23] Ryan Hutson. Manager, Entergy Corporation. Telephone Interview. 25 February 2011.
[24] SAP for Banking: Delivering Solutions for the Dynamic Financial Services Environment. SAP Global. 28 February 2011. http://www.sap.com/industries/ banking
[25] PeopleSoft Enterprise Applications. Oracle. 28 February 2011 http://www.oracle.com/us/products/applications/peoplesoft-enterprise/index.htm
[26] Telephone interview with senior official at the Federal Reserve Board, Washington, DC. 8 March 2011.

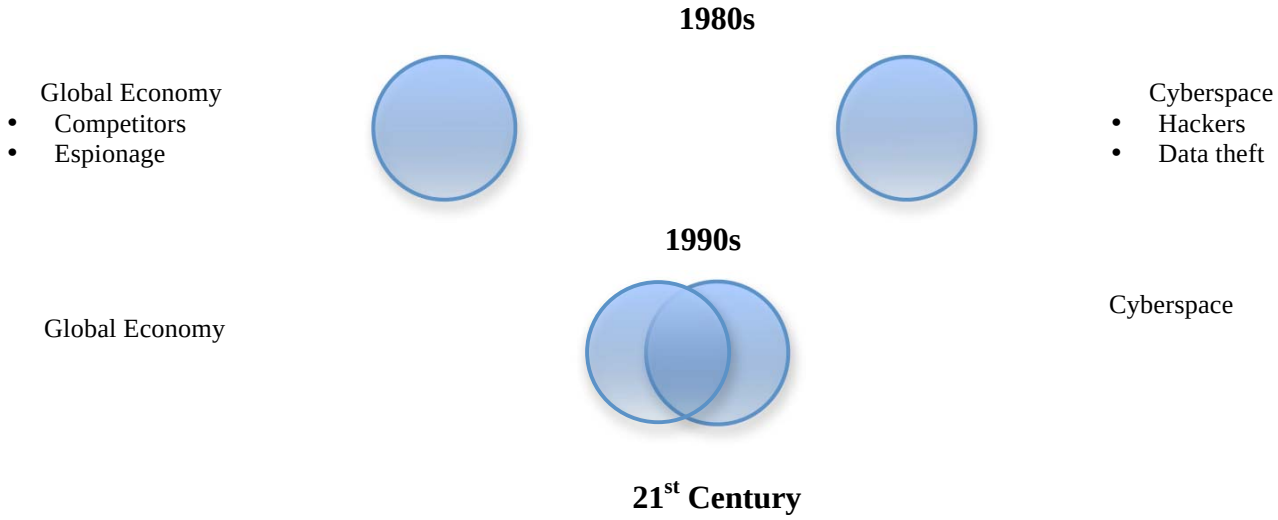
Geography

There is little available information concerning the geographic organization of the Banking and Finance sector as a whole. With close to 10,000 banks and savings institutions in the country, it is a disbursed and fragmented industry.[27] However, the Federal Reserve System is structured and organized geographically into twelve districts, each with a designated Reserve Bank city (shown below).[28,29]



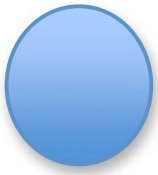
Future Trends

The following diagram depicts the ever-increasing dependence of the global economy on cyberspace. As the Banking and Finance sector evolves, so does its dependence on cyber assets. In the 21st century, they occupy the same space and share risks.[30]



[27] FDIC: Dynamic Depositor Discipline in U.S. Banks. Federal Deposit Insurance Corporation. 12 April 2011. http://www.fdic.gov/bank/analytical/working/wp2003_07/index.html#fig04
[28] FRB: Federal Reserve Districts and Banks. The Federal Reserve System. 12 April 2011. http://www.federalreserve.gov/otherfrb.htm
[29] FRB: Federal Reserve Districts and Banks. The Federal Reserve System. 12 April 2011. http://www.federalreserve.gov/otherfrb.htm
[30] Power, Richard. Cyber Security in the Three Times: Past, Present, and Future. CERT 20th Anniversary Seminar Series. Pittsburgh, PA. 22 July 2008.

Global Economy
- Hackers
- Data theft



Cyberspace
- Competitors
- Espionage

The following specific trends were also identified in a 2008 CERT Seminar Series hosted by Carnegie Mellon CyLab, one of the largest university-based cyber security research and education centers in the United States:[31]

- Increased professionalism and commercialization of malicious activities
- Threats tailored for specific regions and increasing numbers of multi-staged attacks
- Attackers targeting victims by first exploiting trusted entities
- Convergence of attack methods
- Automated evasion process
- Advanced Web threats –laundering origins through the Web
- Diversification of bot usage
- Ratio of non-malicious to malicious software is reaching a tipping point. Levels of malicious code & unwanted programs will exceed number of legitimate software; security techniques will switch from blacklisting to white-listing
- 43% of enterprises have little or no measures in place to address permissions or restrictions on removable media, less than 17% have related end-point security measures; attackers may introduce malicious code at one point or another during manufacture or distribution
- More advanced botnet threats that employ stealth methods such as steganography, allowing botmasters to exploit public forums and search engines
- As U.S. national elections draw near, an increase in phishing, scams and malicious code targeting candidates, campaigns, etc.

Chemical Manufacturing

The Chemical Manufacturing sector combines organic and inorganic materials to make chemicals used in everyday life and that contribute to the national security, public safety, and economic security. The components of this industry are:[32]

- Basic chemicals
- Specialty chemicals
- Agricultural chemicals
- Pharmaceutical
- Consumer products

[31] Power, Richard. Cyber Security in the Three Times: Past, Present, and Future. CERT 20th Anniversary Seminar Series. Pittsburgh, PA. 22 July 2008.
[32] Adam, Nabil. "Workshop on Future Directions in Cyber-Physical Systems Security". *Department of Homeland Security*. January 2010. http://www.ee.washington.edu/faculty/radha/dhs_cps.pdf

Cyber Assets and Functions

The Chemical Manufacturing sector primarily relies on industrial control systems such as distributed control systems (DCS) and supervisory control and data acquisition (SCADA) systems to remotely control manufacturing processes. Chemical manufacturing and production processes primarily rely on DCS, while the pharmaceutical and petrochemical industries use SCADA to monitor and supervise production.[33] The systems monitor tank levels, ensure that chemicals are mixed in the correct proportions, and collect, send, and store data about chemical production.[34] Like other industries, the chemical sector also relies on communication and IT systems that allow users to remotely connect to industrial control systems.

Geography

Chemical facilities are self-contained and not part of a network of manufacturing plants. Industrial control systems in the chemical industry are not interconnected. Thus, the destruction or disruption of a cyber asset at one chemical manufacturing or storage facility would not cause cascading effects across the sector.[35]

Future Trends

Unsecure hardware and software from foreign sources are potential cyber security problem as companies are becoming increasingly reliant on commercial, off-the-shelf (COTS) products.

Commercial Facilities Sector

The Commercial Facilities (CF) sector is primarily focused on maintaining the economic flow of goods and services as well as the safety and security of areas where large numbers of people gather for business and recreational activities. As commercial facilities are highly fragmented and 95% owned by private entities, DHS has acknowledged that prioritization of criticality lies with each owner/operator.[36]

The CF infrastructure is divided into eight subsectors, which consist of Entertainment and Media, Gaming Facilities, Lodging, Outdoor Events, Public Assembly, Real Estate, Retail, and Sport Leagues. They include entities such as "hotels, commercial office buildings, convention centers, stadiums, theme parks, residential buildings, shopping centers, and other sites where large numbers of people gather to pursue business activities, conduct personal commercial transactions, or enjoy recreational pastimes."[37]

---

[33] Adam, Nabil. "Workshop on Future Directions in Cyber-Physical Systems Security". *Department of Homeland Security*. January 2010. http://www.ee.washington.edu/faculty/radha/dhs_cps.pdf
[34] Spellman, Frank and Bieber, Revonna. *Chemical Infrastructure Protection and Homeland Security*. Lanham: The Rowman &Littlefield Publishing Group, Inc. 2009. 40-41.
[35] Ibid, Adam
[36] United States Department of Homeland Security. "Commercial Facilities Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan." (2010): 57.
[37] Ibid 13.

Cyber Assets and Functions

Though not necessary for primary functions, the commercial sector does have cyber systems related to some operations, such as "access control; loss prevention systems; fire and intrusion alarms; communication/dispatch centers; heating, ventilation, and air conditioning systems (HVAC); lighting; closed-circuit television (CCTV); property management; reservations, ticketing, and human resources; and financial management."[38] These can range from basic operating systems, such as SCADA, to dependence upon information technology and communications, but most cyber assets are virtual, rather than hardware, based. The CF infrastructure would be primarily affected if information technology and communications were disrupted, since the CF sector relies heavily on the Internet.[39]

Geography

Each subsector and entity is located a different facility, though facilities may be concentrated in a certain geographical area and therefore rely upon similar resource sources, such as electricity. DHS has acknowledged that a disruption in operations at one facility is not likely to affect operations in another, particularly with cyber assets.[40]

Future Trends

As the CF sector cyber assets are based on information technology and communications, commercial facilities have closely followed the developing trends within both cyber elements in order to improve affordability and effectiveness of the cyber functions listed above. Commercial facilities generally use COTS technology, unlike technology used in controlled environments for other infrastructures.

Critical Manufacturing Sector

According to DHS, the Critical Manufacturing sector includes:[41]

- Primary metal manufacturing (iron and steel mills and ferro alloy manufacturing, alumina and aluminum production and processing, nonferrous metal [except aluminum] production and processing)
- Machinery manufacturing (engine, turbine, and power transmission equipment manufacturing)
- Electrical equipment, appliance, and component manufacturing (electrical equipment manufacturing)
- Transportation equipment manufacturing (vehicle manufacturing, aviation and aerospace product and parts manufacturing, railroad rolling stock manufacturing)

[38] Ibid 20.
[39] Ibid 38.
[40] Ibid 20.
[41] United States. *National Infrastructure Protection Plan: Critical Manufacturing Sector*. 2009.

Cyber Assets and Functions

Manufacturing firms generally use SCADA systems to facilitate production operations. SCADA systems help to collectivize data into one central location from different geographically dispersed entities. This software is used an integral part of the SCADA system for many manufacturing firms in different industries.[42]

Geography

Contemporary production lines are made up of complex interdependent supply chains that span thousands of miles and many times across country borders. One company is connected to numerous other suppliers, vendors, partners, integrators, contractors, and customers, each with their own supply chain networks.[43] This interconnectedness means that a manufacturing company could be affected by cyber attacks on another, remote area of its supply chain. Also, manufacturing firms rely heavily on other sectors of critical infrastructure for their own production, such as communications and energy. If something were to happen in either of those sectors, it could have a profound effect on the Manufacturing sector.

Future Trends

On September 8, 2008, DHS created a new advisory board called Critical Manufacturing Sector Coordinating Council (CMSCC) in conjunction with announcing critical manufacturing as a critical sector. While this is a good initial start to creating a consensus in the industry, so far there are no standards for companies to comply with for cyber protection and there is also no talk of creating such standards. While the large companies that are present in the CMSCC may be able to have sufficient in-house protections, the problems lie in the supply chain. Because there is no oversight committee for the entire manufacturing sector with the power to standardize the needed protection, each firm can decide what level of protection they want for their company.

Recent reports show that the chosen level of protection is falling far below what is needed. According to Symantics, "63 percent [of companies] experienced an outage from cyber attacks over the past 12 months resulting in 52.7 hours of downtime," while "72 percent experienced an outage from system upgrades, resulting in 50.9 hours of downtime."[44] While this data is for small and medium sized businesses, it still shows that although the protective software to prevent these sorts of outages are available, companies along the supply chain are still hesitant to use them. Until standards are placed upon the industry, there is no evidence that this trend will change in the future.

---

[42] Chiappinelli, Chris. "Cyber-attack Threatens Manufacturing Software Systems Worldwide." *Managing Automation*. Managing Automation, 22 Jul 2010. 22 Mar 2011. http://www.managingautomation.com/maonline/news/read/Cyber_attack_Threatens_Manufacturing_Software_Systems_Worldwide_33612

[43] *National Infrastructure Protection Plan: Critical Manufacturing Sector*.

[44] "Virtualization and Cloud Technologies Add Complexity to Disaster Recovery Initiatives." *Symantec 2011 SMB Disaster Preparedness Survey*. Symantic, 22 Nov 2010. 22 Mar 2011. http://www.symantec.com/about/news/release/article.jsp?prid=20101122_01

Dams Sector

The Dam sector includes different subdivisions, such as dam projects, hydropower plants, navigation locks, levees, dikes, hurricane barriers, mine tailings and other industrial waste impoundments, or other similar water retention and water control facilities, and each component uses control systems to either directly or remotely monitor and control the necessary operations.[45] There is often no distinct separation or distinction between the different sectors as they are often combined, connected or somehow related. For example, a dam system may include the dam itself, combined with navigation locks, a hydropower plant, and levees. Therefore, incidents in one area can affect other sectors to some degree.

The dam sector has many functions, depending on the subdivision being analyzed, such as hydroelectric power, river navigation, water supply, wildlife habitat, waste management, flood control, and recreation.[46] However, at its most basic level, the dam sector controls water, including the water's direction, flow, safety, levels, and uses. All other functions are a variation or alteration to that general purpose.

Cyber Assets and Functions

The control systems included with the Dams sector are responsible for two functions: information monitoring and control. These control systems monitor gate position, reservoir level, hydroelectric generator output, and water flow for different infrastructures. This information is then used to either automatically or manually make decisions or determine appropriate actions. The control systems can be further divided into three categories: supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS) and programmable logic controllers (PLC). SCADA systems are typically a centralized group used to manage a variety of systems throughout a location. Conversely, DCS systems are dispersed throughout a site and connected together to form a network. Additionally, DCS systems may directly connect to switches, pumps, and valves or can be controlled through another system.[47] PLC systems are smaller, localized control systems that control specific process at the site. Often, these systems are not used in as a stand-alone component but in an integrated system as part of the whole network.

In addition to the actual control systems, networks and telecommunications equipment are used to transmit, receive and share information from remote points or accesses. This has led to increased use of Virtual Private Network (VPN) tools, access to Internet Protocol (IP) addresses, use of commercial, off the shelf systems such as Windows and UNIX and connectivity with additional internal and external network and will be discussed further in the next section.[48]

[45] United States. Dams Sector Roadmap to Secure Control Systems. 2010. Web. 13 Apr 2011. http://www.damsafety.org/media/Documents/Security/DamsSectorRoadmaptoSecureControlSystems2010.pdf
[46] United States. National Infrastructure Protection Plan: Dam Sector. 2008. Web. 13 Apr 2011. http://www.dhs.gov/xlibrary/assets/nipp_snapshot_dams.pdf

[48] Dalson, Hal, Enrique Matheu, Yazmin Seda-Sanabria, Andres Lopez-Esquerra, and Kristen Baumgartner. "Addressing Cybersecurity Issues for Dams." 13 Apr 2011. http://ussdams.com/proceedings/2010Proc/493-504.pdf

Geography

The Dams sector is spread geographically across the United States with no centralized system or headquarters but is always located near a water source or system. Additionally, the size and scope of the sector varies widely from structures such as the Hoover Dam to smaller, local treatment plants and water holding facilities. The use of cyber assets will typically be positively correlated with the size or complexity of the facility.

Future Trends

In the Dams sector, there are three main trends with regards to control systems. First, control systems are becoming increasingly automated to decrease costs and human errors. While this does decrease the possibility of human error, it also decreases the likelihood that manual oversight can detect or prevent incidents. Therefore, incidents may go uncorrected or unnoticed for longer. Secondly, commercial or standardized products are becoming more commonplace in the dam sector. As stated above, these include COTS products, like Windows and UNIX, and other systems which increase the possibility that an access point or entrance can be discovered and exploited. Additionally, the integrity of purchased software is often harder to verify and control. Finally, the last trend occurring in dam control systems is interconnectedness. This includes interconnectedness between systems, networks and with the internet.

Defense Industrial Base Sector

The Defense Industrial Base (DIB) sector is focused on the Department of Defense (DOD) and private sector international industrial complexes that contribute research and development, production, and maintenance of military weapons systems and other components necessary to meet U.S. military objectives.[49] It is defined by its customer (DOD), rather than the products themselves and may also overlap with other infrastructure sectors.[50] DHS defines the DIB as entities who produce "defense-related products and services…[which] equip, inform, mobilize, deploy, and sustain forces conducting military operations worldwide," though it does not include elements such as power, communications, transportation, and other utilities that the military may require to conduct operations.[51] Over 85% of the DIB is owned and operated by the private sector, and it consists of over 250,000 separate sites and facilities.[52] DHS separates the DIB into ten segments: missile, aircraft, troop support, space, combat vehicle, ammunition, weapons, information technology, shipbuilding, and electronics.[53] These segments are further broken down into commodities produced under each: mechanical, structural, electrical, and electronics. Companies within the DIB are divided into prime contractors, which actually receive DOD contracts, and subcontractors who produce important subsystems of final military products.[54]

[49] "Defense Industrial Base: Critical Infrastructure and Key Resources Sector-Specific Plan as input to the National Infrastructure Protection Plan." Department of Homeland Security. May 2007: 4.
[50] Ibid 13.
[51] Ibid 5.
[52] Salesses, Robert. "Defense Industrial Base Conference Overview & Objectives," Office of the Secretary of Defense for Homeland Defense and Americas' Security Affairs. 11 Apr 2007: slide 10.
[53] DHS 5.
[54] Hare, Forrest, and Jonathan Goldstein. "The interdependent security problem in the defense industrial base: An agent-based model on a social network." International Journal of Critical Infrastructure Protection. 3. (2010): 131.

Cyber Assets and Functions

The DIB utilizes many of the same cyber assets as the Critical Manufacturing sector, relying primarily on computer-aided design (CAD) software and computer-aided manufacturing (CAM) processes.[55] The companies themselves must also rely on more networked enterprise management and information security systems. Though cyber assets are used primarily for the design and production of military components, the DIB's design specifications, contract information, U.S. Securities and Exchange Commission (SEC) filings, and other proprietary information must be kept secure using tools like encryption and firewalls.

Geography

The DIB sector contains primarily geographically isolated facilities as most do not require a networked infrastructure in order to perform their basic functions. Each is located within an isolated facility, though facilities may be concentrated in a certain geographical area and therefore rely upon similar resource sources, such as electricity. The Department of Energy (DOE) states that "the DIB is best characterized as a loose confederation of assets where impacts of loss or damage tend to be discrete" in physical terms.[56]

Future Trends

Because elements of the DIB are subject to economic competition, the DIB has closely followed the developing commercial trends of cyber elements in order to improve affordability and effectiveness of the cyber functions listed above. Due to the sensitive nature of many DIB products, contractors and vendors are occasionally required to develop, use, and support software that has been completely developed within the United States with vetted U.S. citizens.[57] This is known as "custom software," developed for government use, which is only intended for a single user. On the other hand, mass-produced COTS software and hardware is inherently cheaper, though less secure because of a wider knowledge base of its components.[58] Because of a heavy reliance upon the private industry for military goods and services, the DOD has shown to be "intentionally trading off confidence in the assurance of the critical application for the cost, performance, and availability benefits of COTS."[59] This trend, though improving efficiency and effectiveness, also creates more access and points for malicious users to disrupt or access DIB systems.

Emergency Services Sector

The Emergency Services sector comprises a variety of first responder services in a highly collaborative and integrated system that serves as the United States' first line of defense in the face

[55] "Report of the Defense Science Board Task Force on Mission Impact of Foreign Influence on DoD Software." Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, Department of Defense. September 2007: 72.
[56] DHS 17.
[57] Report of the Defense Science Board Task Force 38.
[58] Ibid 38.
[59] Ibid 40.

of danger and disaster.[60] The services involved in the sector's critical missions include fire, emergency medical services, law enforcement, state and local government officials involved with incident command like the emergency manager, specialized rescue groups, and 911 call centers.[61] These are the first responders in charge of mitigating consequences of natural disasters, accidents, and physical attacks. In recent years, terrorists have demonstrated through physical attacks that the emergency services, too, can fall victim to both deliberate direct and secondary attacks.

Cyber Assets and Functions

The Emergency Services sector is unique in that the critical mission is not based on or produced by a facility, but rather the focus and criticality lie in personnel and equipment. Taking a closer look at the steps taken in response to an emergency, it becomes clear that the sector has shifted to Internet protocol (IP) networks for services like interoperable emergency communications and the 911 call systems. While this shift provides state and local responders new capabilities for response and recovery duties, it also increases dependencies on clear and quick computer-assisted communication.[62] Initially, a witness or victim must report an incident to the authorities and typically a call is placed to a 911 center. The 911 center must have software that can trace a call and provide an address if the caller is unable to provide this information. Call dispatch software is also necessary to link relevant agencies and communicate where they must go and what to expect. When additional resources are needed, those must be called in. A database containing pertinent information is another necessary cyber asset. First responders in the field often use laptops, cell phones, radios, wireless PDAs, and IP phones for coordination, communicating with headquarters, communicating with colleagues at the scene, communicating with other agencies on the scene, and, in a disaster, communicating with incident command. Effective telecommunications capabilities are essential. Playing a supporting role, access and transport for databases and information distribution applications like the I Am Alive (IAA) system are also helpful for smoothly managing a crisis or disaster.[63]

Geography

The Emergency Services sector is not housed in a single facility, but is made up of a variety of services, like EMTs, fire fighters, and police, whose personnel and equipment are housed in multiple facilities. Each town, when size is not prohibitive, maintains its own fire station, hospital, and police stations. So, these facilities may or may not be next door to each other and typically are separated by a matter of blocks or miles. Specialties like hazardous material certified response teams or rescue diving certified response teams are typically shared regionally. Training and equipment cost too much for each town, even for larger cities, to maintain all types of specialized response teams. Instead, often towns within a certain area or region will collaborate and share resources. If one town specializes in one area, a neighboring town will specialize in

[60] "National Infrastructure Protection Plan: Emergency Services Sector." Department of Homeland Security. Accessed February 26, http://www.dhs.gov/nipp
[61] "A Military Guide to Terrorism…," pp. II-3- II-4.
[62] "Cyber Security Guidance." FEMA. Accessed February 2011, https://www.fema.gov/pdf/government/grant/hsgp/fy09_hsgp_cyber.pdf.
[63] This database allows survivors to register, providing a way for family and friends to check on loved ones without burdening the busy workers in the emergency sector. "Internet Emergency Preparedness." Accessed March 2011. http://datatracker.ietf.org/wg/ieprep/charter/

something different, and both towns agree to offer assistance when their specialty is needed. Groupings of these emergency services, whether by town or greater region, exist all over the country. While these services span the nation like the postal sector, unlike the common network effect created by one postal system, emergency services operate independently in each town or region. For example, if the cyber network of a fire station in a suburb of Houston, were penetrated, the intruder could not access employee information at a fire station in Detroit. Damage can often be limited in the compartmented environment.

Future Trends

While there are no trends in the future cyber assets of emergency services, the dependency upon them is growing. Different regional and local responders are integrating their training while becoming more specialized in their work. For example, two neighboring counties may agree to have one of them dedicate a majority of its funding, manpower, and training to HAZMAT mitigation while the other devotes a similar majority of its resources to emergency diving operations. Additionally, they both agree to respond to a particular type of emergency in each other's traditional area of responsibility. In these arrangements, cyber assets, including communications infrastructure, become more important because the dependence upon them increases

Energy Sector

The energy industry produces and distributes electricity, petroleum and refined petroleum products, natural gas and alternative fuel sources. For the purposes of this project, electricity, petroleum and natural gas production and distribution are essential to preserve national security, public safety and economic security, all of which rely heavily on energy and electricity infrastructure. Furthermore, electricity, petroleum and natural gas industries all rely on cyber assets heavily, particularly control, IT and communications systems.

Cyber Assets and Functions (Electricity)

Electricity production utilizes many cyber assets that are essential for the industry to function. These include:

- Control systems (SCADA, DCS, etc.) that manage, command or regulate processes within the facility
- Data acquisition programs including sensors and communication links that collect and provide data from the control systems and relay data back to a centralized location within the facility for display, archiving or further processing
- Networking equipment such as routers, hubs, switches, firewalls and modems
- Hardware platforms[64]
- Telecommunications systems for distribution and production, and
- Commodity IT trading platforms that coordinate the scheduling of power[65]

[64] "Security Guideline for the Electricity Sector: Identifying Critical Cyber Assets". NERC. 17 June 2010. http://www.nerc.com/fileUploads/File/Standards/Critcal%20Cyber%20Asset_approved%20by%20CIPCl%20and%20SC%20for%20Posting%20with%20CIP-002-1,%20CIP-002-2,%20CIP-002-3.pdf

Geography

The U.S. electrical grid is divided into three regions, so a failure in one region would have limited cascading effects on others. However, there is some degree of interconnectivity between regions. There are a total of 152 regional "control areas" that divide the interconnections between the grids.[66] In the event of a coordinated physical and cyber attack of major electrical generators, the U.S. could plausibly experience cascading failure of electricity production for up to two years. However, this is a highly improbable scenario.[67]

Future Trends

The future of electricity generation and distribution will increasingly rely on cyber assets. The U.S. is considering moving to a "smart grid" system in which electricity customers can monitor the amount of power they are consuming using automated meters. These meters will use two-way communications systems and advanced sensors to relay data from producers to consumers. The transition to an even more digitized system for electricity transmission and distribution will impact the cyber security of the electricity sector significantly. Hackers could potentially control thousands to millions of meters, tamper with the data and shut them all off simultaneously. Disrupting the load balance and tampering with the data indicating the demand of power could cause blackouts over large geographical areas and have cascading effects on other parts of the grid.[68]

Cyber Assets and Functions (Petroleum/Natural Gas)

Petroleum and natural gas production and distribution relies on the following cyber assets:

- Control systems for pipelines including SCADA and process control systems (PCS)
- IT systems for data storage[69]

SCADA systems for oil and gas pipelines consist of three primary components: centralized monitoring and control (for the collection and storage of data), communications infrastructure (for transferring data using satellites, bandwidth and dial up systems), and field site devices (for monitoring local processes).[70] These systems are also used in drilling and refining of oil and gas.[71]

---

[66] Adam, Nabil. "Workshop on Future Directions in Cyber-Physical Systems Security". *Department of Homeland Security*. January 2010. http://www.ee.washington.edu/faculty/radha/dhs_cps.pdf

[68] Meserve, Jeanne. "'Smart Grid' may be vulnerable to hackers". CNN. March 20, 2009. http://articles.cnn.com/2009-03-20/tech/smartgrid.vulnerability_1_smart-grid-power-grid-blackout?_s=PM:TECH

[69] A Comparison of Oil and Gas Segment Cyber Security Standards (2004). http://www.us-cert.gov/control_systems/pdf/oil_gas1104.pdf

[70] "Control Systems Cyber Security for the Natural Gas Pipeline Industry". *INGAA*. January 31, 2011. http://www.aga.org/our-issues/security/Documents/INGAAControlSysCyberSecGuidelinesREV.pdf

[71] Spellman, Frank and Bieber, Revonna. *Chemical Infrastructure Protection and Homeland Security*. Lanham: The Rowman &Littlefield Publishing Group, Inc. 2009. Pp 109.

Geography

Oil and gas production consists of the interconnected wells, pipeline networks, refineries, and terminals. There are five divisions within the oil and gas industry that illustrate geographical distribution:

- Exploration and Production (Upstream) – Oil and gas wells and drilling sites are dispersed around the country, both on and off-shore. There are over 500,000 producing wells and 3,800 oil and natural gas platforms off-shore.
- Refining and Marketing (Downstream) – 141 U.S. refineries process oil and gas into other energies. This is then transported to terminals and service stations by tanker trucks.
- Pipeline – 165,000 miles of pipeline transport oil and gas from the wells and platforms to the refineries, terminals and retail outlets.
- Marine – oil tankers and other vehicles transport oil and gas products by water.
- Service and Supply – the equipment, design, services and engineering support necessary for the production of energy are dispersed throughout the nation.[72]

There are also various storage facilities for oil and gas. Electricity power plants rely on oil and gas pipelines as a source of fuel. The infrastructure is an integrated web of production, transportation and refining, most of which is connected to cyber assets.

Future Trends

Oil and gas producers are researching and implementing new technologies in order to exploit resources that were previously uneconomical to mine. The DOE is also devoting significant resources to the maintenance and expansion of oil and gas pipelines. High tech devices monitor existing underground and aboveground pipes to signal the need for any repairs. This increased capacity in the pipeline system will require cyber components and control systems to monitor the transmission, distribution, and storage of energy.[73]

Government Facilities Sector

According to DHS, the Government Facilities sector of U.S. critical infrastructure encompasses federal, state, local, and tribal agency headquarters buildings, general use office buildings, courthouses, over 87,000 municipal government buildings, national laboratories, military installations, and diplomatic missions, embassies, and consulates abroad.[74] Since these facilities are home to federal, state, local, and tribal government entities, it is no surprise that this is where governmental functions are performed every day. At the federal facilities, agencies and individuals communicate with one another to share information and collaborate on products for consumers. They process, analyze, and disseminate intelligence, coordinate military operations,

[72] American Petroleum Institute. "Industry Sectors". March 31, 2011. http://www.api.org/aboutoilgas/sectors/index.cfm
[73] Deparment of Energy. "Transmission, Distribution and Storage". 23, January 2009. http://www.fossil.energy.gov/programs/oilgas/delivery/index.html
[74] United States Of America. Department of Homeland Security. Office of Infrastructure Protection. *National Infrastructure Protection Plan Snapshot: Government Facilities*. DHS, 2009. 15 Feb. 2011. http://www.dhs.gov/xlibrary/assets/nipp_snapshot_governmentfacilities.pdf

conduct negotiations and investigations, and address public grievances. Government facilities, in turn, are essential to the national security, economic security, and public safety apparatuses because those facilities house the decision makers of national, state, local, and tribal government policies.

Cyber Assets and Functions

Like much of society, government facilities rely heavily on assets with a cyber component for their daily operation in today's digital age. Examples of such assets include computers with Internet access, open source and classified databases, extensive communication systems (sometimes referred to as *ad hoc* communication systems), and access control systems.[75,76] Often, these cyber components are managed via an enterprise application system (EAS), which allows the assets to help government facilities perform their daily functions.

Each of these assets serves a purpose that contributes to the daily operation of the facilities and the conduct of federal, state, local, and tribal government business. Almost all government agencies maintain a website to update its constituency on the latest pertinent information. Every day, government employees at home and abroad use open source and classified databases to run checks on suspected persons of interest, verify potential intelligence sources, corroborate data, aggregate information, and conduct research to help formulate policy decisions. Federal, state, local, and tribal government employees rely on different systems of email, telephone, and fax to communicate information, organize projects, and conduct daily affairs.[77] These day-to-day systems fit under the broad term of enterprise application software.[78] Access control systems requiring combinations of identification (ID) badges, personal identification numbers (PINs), and biometric data prevent unauthorized entry and exit of unauthorized people and materials into and out of the facilities. Alarm systems, security cameras, motion detectors, closed-circuit television (CCTV) and other sensors, in tandem with armed security guards, prevent unauthorized personnel and materials from accessing the facilities.[79]

Geography

Government facilities are located across the United States and the world. While federal government facilities are located primarily in the Washington, D.C. metropolitan area, there are also many embassies and consulates located in major cities throughout the world that communicate with headquarters every day. State, local, and tribal governments are located in their respective state capitals and urban areas. Their cyber assets are also not inherently linked. For instance, an attack on State Department computers would not necessarily affect computer

[75] Interview with James Olson, Lecturer, Bush School of Government and Public Service. College Station, TX. 22 February 2011.
[76] Interview with Ambassador (ret.) Larry Napper. Professor and Director of the Scowcroft Institute, Bush School of Government and Public Service. College Station, TX. 2 February 2011.
[77] Interview with James Olson, Lecturer, Bush School of Government and Public Service. College Station, TX. 22 February 2011.
[78] "Enterprise Software." Capterra. 2010. http://www.capterra.com/enterprise_software_definition
[79] Interview with Ambassador (ret.) Larry Napper. Professor and Director of the Scowcroft Institute, Bush School of Government and Public Service. College Station, TX. 2 February 2011.

networks at the Department of Justice. This may help to mitigate the consequences of a concentrated cyber attack.

Future Trends

The extent to which government facilities and the U.S. military depend on cyber assets is growing. According to a June 2010 GAO report called "Continued Attention Is Needed to Protect Federal Information Systems from Evolving Threats," almost all government operations are supported by automated systems and many agencies would have a very difficult time conducting daily functions without them.[80] Additionally, federal agencies like DHS are beginning to use social media to communicate with the public. This is being done to share information regarding threat levels and promote accountability and transparency in DHS operations.[81] While government facilities will likely still depend heavily on enterprise application software, the dependence is increasing. Social networking websites will also become an asset they use primarily for communication with the public.

National Monuments and Icons Sector

The National Monuments and Icons sector includes a variety of assets of varying importance, size, and location. However, according to the sector overview from DHS, all the assets of this sector have three common characteristics:[82]

- They are a monument, physical structure, object, or geographic site
- They are widely recognized to represent the nation's heritage, traditions, or values, or widely recognized to represent important national cultural, religious, historical, or political significance
- Their primary purpose is to memorialize or represent some significant aspect of the nation's heritage, tradition, or values, and to serve as points of interest for visitors and educational activities.

Cyber Assets and Functions

For the scope of our project, we have not included the National Monuments and Icons sector in analysis because national monuments and icons do not rely on computer or internet-based systems to function.

[80] "Cybersecurity: Continued Attention is Needed to Protect Federal Information Systems from Evolving Threats." Statement of Gregory C. Wilhusen, Director, Information Security Issues. Government Accountability Office. 16 June 2010. http://www.gao.gov/new.items/d10834t.pdf

[81] "Privacy Impact Assessment for the Use of Social Networking Interactions and Applications Communications/Outreach/Public Dialogue." U.S. Department of Homeland Security. 16 September 2010. http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_dhs_socialnetworkinginteractions.pdf

[82] United States. National Infrastructure Protection Plan: National Monuments and Icons Sector. , 2008. 17 Apr 2011. http://www.dhs.gov/xlibrary/assets/nipp_snapshot_nationalmonuments.pdf

Geography

National monuments and icons are located in clusters throughout the United States, especially in areas of large population and of historical significance.

Future Trends

There are no significant foreseeable changes in the National Monuments and Icons sector.

Nuclear Reactors, Material, and Waste Sector

The Nuclear Reactors, Material, and Waste (NRMW) sector is focused on maintaining safe energy production as well as ensuring that radiological materials are secure and used for their intended purposes. The DHS has identified the NRMW sector as being closely linked with the energy, transportation (of radiological materials), chemical (by-products from fuel-cycle and industrial activities), public health and healthcare (medical uses), and government facilities critical infrastructures.[83]

The NRMW sector comprises of a wide range of sectors related to energy production as well as the development, use, and transportation of radiological materials. The sector focuses on commercial nuclear power plants, which produce about 20 percent of the country's electricity.[84] Currently, the United States has 104 operating commercial nuclear power plants in 31 states, including 35 boiling water reactors and 69 pressurized water reactors. The Nuclear Regulatory Commission (NRC) is the primary body which regulates the commercial nuclear power industry, and it also oversees the production and transportation of "source material," or nuclear fuel and necessary material components, which originate from uranium and other ore mining, reprocessing spent fuel, and depleted uranium from the enrichment process.[85]

The NRMW also focuses on research and test reactors, which are used for development, training, and research purposes. The NRC oversees 32 operating reactors and 9 other reactors, which are either being decommissioned or are not in operation, and the majority of these research and test reactors are located on college and university campuses across the United States. Also, the Department of Energy also operates several research and test reactors to study new designs and fuel cycle properties.[86]

In addition to reactors, the NRMW also entails radioactive materials used in medical, industrial, and academic settings. Radioactive materials are used for monitoring, imaging, and treating metabolic tissues and processes within humans as well as animals; industrial systems such

[83] "National Infrastructure Protection Plan: Nuclear Reactors, Materials, and Waste Sector." *Department of Homeland Security*. 14 Jan 2010. Retrieved 12 Apr 2011. http://www.dhs.gov/xlibrary/assets/nipp_snapshot_nuclear.pdf
[84] "U.S. Nuclear Power Plants." *Nuclear Energy Institute.* Retrieved 12 Apr 2011. http://www.nei.org/resourcesandstats/nuclear_statistics/usnuclearpowerplants/
[85] "Source Material." *Nuclear Regulatory Commission*, 12 Feb 2007. Retrieved 14 Apr 2011. http://www.nrc.gov/materials/srcmaterial.html
[86] "Research and Test Reactors." *Nuclear Regulatory Commission*, 16 Mar 2011. Retrieved 13 Apr 2011. http://www.nrc.gov/reactors/non-power.html

as irradiators, well-logging devices, radiography systems, and gauging devices; and classroom, laboratory, and research purposes at academic institutions.[87]

Finally, NRMW includes the transportation, storage, or disposal of radioactive waste. Radioactive waste ranges from low-level waste from contaminated items to high-level waste from spent nuclear fuel. Certain by-products, such as uranium tailings and residues after ore mining or waste byproducts from reprocessing are also included.[88]

Cyber Assets and Functions

NRMW utilize several cyber assets to monitor and operate equipment; perform safety, security, and emergency preparedness function; and compute and store data. These include analogue systems, which are "hard-wired" to perform functions, and digital computer-based systems, which use software stored in memory.[89]

Common cyber assets include supervisory control and data acquisition (SCADA) systems used for monitoring and operating processes within nuclear reactors and industrial production as well as distributed control systems, which primarily control the flow of electricity from nuclear power plants to the electrical grid. Many of these systems are isolated from networks like the Internet, though some are currently linked to the same computers and servers used for administrative purposes.[90] Cyber assets that perform lesser functions include administration and enterprise systems and information technology and communications to perform business-related functions.

Geography

The NRMW critical infrastructure contains both geographically isolated facilities and networked entities. Research and test reactors, radioactive materials, and nuclear waste themselves do not require a networked infrastructure in order to perform their basic functions; each is completed within an isolated facility, though facilities may be concentrated in a certain geographical area and therefore rely upon similar resource sources, such as electricity. Nuclear power plants, however, are a component of the electrical grid network, which spreads across a wider geographical area outside the facility itself. See the "Energy Critical Infrastructure" section on page 21 for a more in-depth description of this distribution.

[87] "Medical, Industrial, and Academic Uses of Nuclear Materials." *Nuclear Regulatory Commission*, 16 Sep 2009. Retrieved 13 Apr 2011. http://www.nrc.gov/materials/medical.html
[88] "Radioactive Waste." *Nuclear Regulatory Commission,* 7 Jan 2011. Retrieved 13 Apr 2011. http://www.nrc.gov/waste.html
[89] "Backgrounder on Cyber Security." *Nuclear Regulatory Commission*, 1 Apr 2010. Retrieved 14 Apr 2011. http://www.nrc.gov/reading-rm/doc-collections/fact-sheets/cyber-security-bg.html
[90] Matishak, Martin. "Nation's Nuclear Power Plants Prepare for Cyber Attacks." Global Security Newswire, Nuclear Threat Initiative (27 Aug 2010): Retrieved 14 Apr 2011. <http://gsn.nti.org/gsn/nw_20100827_1692.php>.

Future Trends

Cyber assets, especially in the expanding commercial nuclear power plant sector, are being updated to become more interoperable, remotely accessible, and less costly.[91] Plans for new commercial reactors have shown an increased "reliance on digital control systems," and current plants and other industrial facilities are retro-fitting existing systems to remain competitive.[92] In addition, nuclear power plants and industrial/material production facilities are also following the overall trend of becoming increasingly linked through wireless information technology and communications to "multiple sites, mobile plant employees, corporate staff, vendors providing outsourced services, and even government agencies" overseeing compliance with regulations.[93] Because of the recognized increased vulnerability of increased networking and outside connections, the Nuclear Regulatory Commission and the North American Electric Reliability Corporation are instituting new guidelines, such as the "Protection of Digital Computer and Communications Systems and Networks" (10 CFR 73.54), which requires new measures to protect from cyber attack or human error those cyber assets associated with "safety-related and important-to-safety functions, security functions, emergency preparedness functions, including offsite communications, and support systems and equipment important to safety and security."[94]

Postal and Shipping Sector

The United States Postal Service (USPS) maintains the country's largest operating intranet.[95] USPS transactions contribute to a significant portion of the U.S. economy. These reach more than 137 million addresses across the country and require around 300,000 carriers.[96] This network infrastructure of USPS maintains more than 185,000 workstations and more than 10,000 servers. USPS is interconnected with other infrastructure systems, like transportation, energy, and IT/communications. These linkages allow USPS to transport over half a billion pieces of mail daily, power its facilities and operations, and use operating systems to record deliveries and shipments. The postal sector also handles sensitive materials like passport applications. As a result, the postal service attracts cyber criminals and is a target for actors engaging in industrial espionage and economic and technological competition.[97] If the USPS functions were to lag, or worse yet, stop, ramifications would reach far and be nationally significant. The lead agency in charge of informing the postal sector of current or imminent threats is the Department of Homeland Security.[98]

---

[91] Hurst, Timothy. "Time to get serious about security." POWER Magazine (15 Apr 2008): Retrieved 14 Apr 2011. http://www.powermag.com/smart_grid/Time-to-get-serious-about-security_69.html
[92] Matishak.
[93] Hurst; Flowers, James. "I&C Update on Plant Vogtle Units 3 and 4." POWER Magazine (1 Feb 2011): Retrieved 14 Apr 2011. http://www.powermag.com/nuclear/3389.html
[94] "Backgrounder on Cyber Security."
[95] "Cyber Intelligence Division Works Across Borders," Postal Inspection Service News. June 2008. Pg. 2.
[96] "A Military Guide to Terrorism in the Twenty-First Century," US Army Training and Doctrine Command (August 2006). Fort Leavenworth. p. II-9.
[97] Aliya Sternstein, "Postal Service IG Examines Cyber Incident Data." Next Gov: Technology and the Business of Government. November 2010. Pg. 1.
[98] "Technology Assessment: Cyber Security for Critical Infrastructure Protection," General Accounting Office. May 2004. Pg. 101.

Cyber Assets and Functions

The postal sector relies on cyber assets at nearly every step in the execution of its mission, from the point of sales to the delivery of the mail to its destination, as well as in supporting roles for maintenance of these capabilities. USPS relies on highly automated distribution and scheduling systems for rail transport, air mail, and truck delivery. Multiple computer functions and systems are used at each step of the mail delivery process. For example, there are a variety of postage payment methods and barcoding systems and methods. One such system is the Manifest Mailing System, an automated way of verifying postage payment of imprint mailings. Consumers must purchase a software system that meets the Express Mail Manifesting requirements.[99] Another example of cyber assets facilitating the logistical process is found at processing and distribution centers. Upgraded conveyor systems use individually powered intelligent rollers connected by computer to control modules and photo-electronic sensors through a Smart Distributed System intelligent bus network and a Smart Control System from a nearby center. Using this retrofitted system, plastic trays transport mail along the conveyor including more than one hundred curves and lane changes. The system uses scanners to read bar codes on the tubs to sort and guide them according to their destinations. These scanners are also linked to a central computer.[100] While these examples are not comprehensive, they demonstrate the intricate dependency of the postal sector on cyber assets in every function required for the success of the critical mission, getting letters from a point of origin to a destination promptly.

Geography

The USPS spans the entire country, connecting every town, village, business, and home. As previously mentioned, the postal sector is comprised of 185,000 workstations, with a post office in every town and multiple post offices in most metropolitan areas. This service enables more than 300,000 carriers to transport and communicate goods to more than 137 million addresses across the country.[101] The dispersed nature of the postal sector presents two very different implications, depending on one's perspective. First, because structures are not concentrated in one area, the impact of cyber attacks might be compartmentalized or only affect an isolated facility. If an attacker hacked into a physical security system at a small town post office, the repercussions may be contained. Second, and potentially more serious, if an outsider gained access to a customer databank at a distribution center, hundreds of thousands of Americans' personal information could be exposed.

Future Trends

One of the most common ways an intruder can gain access to this system is by directly dialing modems attached to field equipment.[102] War dialing is a computer program designed to

[99] "P910 Manifest Mailing System (MMS)," P900 Special Postage Payment Systems, http://pe.usps.com/archive/html/dmmarchive0810/P910.htm, pp. 1,7.
[100] For more on this particular conveyor upgrade system, see Jim Butschli, "USPS Ups Efficiency with 'Smart' Conveyor Controls," Packaging World. October 1997, pg. 1.
[101] "A Military Guide to Terrorism in the Twenty-First Century," US Army Training and Doctrine Command (August 2006). Fort Leavenworth. p. II-9.
[102] Ibid. Pg. 6

locate telephone numbers that can connect with a computer modem.[103] Using this technique, an intruder could access the postal service's intranet, if successful, undetected. They usually target unsecure or unauthorized modems. Resulting cyber attacks could compromise the integrity and the confidentiality of USPS.[104] Risks like this deem modem security imperative to the security of the entire postal sector. Policy strictly forbids accessing the USPS's intranet through a modem that has not been approved by the manager. Careful inventory of modems and modem security assessments are both ways the postal sector can improve control and reduce this area of vulnerability.[105]

Public Health Sector

Although the public health care system is a vital part of America's infrastructure, the main cyber problems that the industry seeks to address are unrelated to patient health. Instead, they deal with the protection of patients' identities and protecting patent rights. The functions of the industry that are most likely to be disrupted by a cyber attack are the integrity of patient's records, billing, and securing notifications to the correct patient. There are growing concerns about the potential for more life threatening consequences from cyber attacks. Computers have had an increasingly prominent presence in the practice of medicine over the past few years, which has increased the connectivity of systems considered to be necessary for healthcare. These cyber assets engage in many of the primary functions for a hospital. They are used to monitor patients, distribute medication, and operate life support systems.[106]

Cyber Assets and Functions

There are numerous programs available to help protect the data collected by healthcare entities and the flow of this information. More than one of the following programs are used and the combination of different systems creates a secure network with multiple fail safes in place to fully control access to the data.[107]

- Security Risk Assessments – a process that compares the controls in place to the regulatory requirements, and determines if there are any gaps. The assessment also compares the organization's system with other companies in the industry.

- Intrusion Prevention and Detection Services (IPS/IDS) – systems that detect and block attempts made by cyber criminals to access data on the server and network. They alert the server manager to attempted cyber attacks and allow them to respond in real-time.

---

[103] Deborah Judy, "Audit Report: Modem Security of the [classified]," Report Number: IS-AR-10-009. Office of the Inspector General. Pg. 4.

[104] Cyber terrorists or intranet intruders generally have three basic goals they can accomplish by entering cyber space in which they do not belong. These goals include compromising an entity's cyber integrity, its availability, and its confidentiality. For more, see: "A Military Guide to Terrorism…," p. VII-3.

[105] Judy, "Audit Report…," pp. 1 & 7.

[106] McBride, Michael. "Cyber-Attacks against Internet-Enabled Medical Devices are New Threat to Clinical Pathology Laboratories." *Dark Daily*. Dark Daily, 16 Feb 2011. 7 Apr 2011. http://www.darkdaily.com/cyber-attacks-against-internet-enabled-medical-devices-are-new-threat-to-clinical-pathology-laboratories-215

[107] "Hacker Attacks Targeting Healthcare Organizations Doubled in the 4th Quarter of 2009 according to Dell SecureWorks' Data."

- Data Loss Prevention (DLP) – systems that monitors network traffic for possible leakage of personal identification information (PII), such as social security numbers and protected health information (PHI), such as Health Level 7 (HL7) codes (medical standards/procedures codes).

- Log Monitoring – function which centralizes and correlates audit logs from applications and systems. This allows the owners to identify improper access to sensitive patient data from internal or external sources.

- Web Application Security Testing and Web Application Firewalls – Because of the prevalence of web applications available to healthcare customers, these portals need to be fully protected from external attacks. By performing regular web application security testing and implementing a web application firewall, this aspect of the network can be protected.

- Encryption – Numerous devices are used by almost everyone involved in the healthcare industry so implementing strong encryption policies and technologies on all mobile devices, laptops, portable storage and backup tapes would help to protect all devices from improper data disclosure regardless of where they are or who is using them.

Geography

While a hospital may appear to be a small area to protect, they are located in almost every major town and city across the nation. Additionally, healthcare organizations have to stay in contact with patients, employees, insurers, and business partners. Each of these individuals has to have a way to access healthcare information, which opens the network to human errors and exploitable external ports.[108]

Future Trends

In late 2009, Congress put into place a new regulation called the Health Information Technology for Economic and Clinical Health Act, or HITECH, that was intended to boost the cyber security of the industry. It was entirely geared towards identity theft and specifically included two rules which expanded the reach of the security measures already in place. The first is a privacy rule that refers to all PHI in both electronic and paper format and the other is a security rule, which deals specifically with Electronic Protected Health Information (EPHI).[109]

> Section 13402 of the Act requires HIPAA covered entities to notify affected individuals, and requires business associates to notify covered entities, following the discovery of a breach of unsecured protected health information (PHI).

[108] "Hacker Attacks Targeting Healthcare Organizations Doubled in the 4th Quarter of 2009 according to Dell SecureWorks' Data." *Dell Secureworks*. Dell, 26 Jan 2010. 27 Feb 2011. http://www.secureworks.com/media/press_releases/20100126-healthcare-attacks/

[109] "Health IT." *The Office of the National Coordinator for Health Information Technology*. Department of Health Services, 28 Feb 2011. 27 Feb 2011. http://healthit.hhs.gov/portal/server.pt/community/healthit_hhs_gov__home/1204

> Section 13407 of the Act defines "unsecured PHR identifiable information" as personal health record (PHR) identifiable health information that is not protected through the use of a technology or methodology specified in the Secretary's guidance.[110]

The legislature mostly concerns itself with what to do when a breach occurs, however the Secretary did release a supplementary guidance on what the entities that fall under this jurisdiction should do. The guidance covers physical, administrative, and technical precautions that the Department of Health and Human Services recommends. For specifically cyber assets, the technical protections endorsed are audit controls, audit controls, integrity controls, and transmission security.[111] Many of the security systems mentioned before fall under these guidelines that should be used for the health organization to avoid the ramifications that come from the new HITECH legislature.

In response to the danger cyber attacks pose to actual medical equipment, hospitals have begun to separate these machines from the main hospital network. They can function as their own entity without the fear of being brought down in a crippling attack. This does cause logistics problem for hospitals, but it appears to be a workable solution.[112]

Transportation Sector

According to the DHS, the Transportation sector of critical infrastructure encompasses aviation, maritime, mass transit, railway, highway, and pipeline transportation networks. However, for the scope of this project, pipeline infrastructure has been designated as part of the energy sector to avoid overlap and repetition of analysis. Thus, transportation will refer only to modes of transport for human beings and materials that are not moved via pipeline.

The degree to which transportation modes rely on cyber assets varies. For instance, the air traffic control grid is more technologically robust than assets related to the highway system. Nevertheless, it is necessary to examine each mode of transportation to determine what the transportation cyber assets are and develop a solid understanding of their functions.

Aside from basic electric components on board a particular transportation vessel, many modes of transportation rely on SCADA systems to control dispatches, coordinate arrivals, and monitor assets.[113] Transportation industries have also developed Information and Analysis Centers (ISAC), which allow relevant agencies and entities to quickly share information about emerging threats, outages, and vulnerabilities. The modes also have a publicly accessible interface by which important information can be relayed to the public.

---

[110] Johnson, Charles. "Guidance Specifying the Technologies and Methodologies." *Covered Entities for Security Rule*. Health and Human Services, 25 Apr 2011. http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/hitechrfi.pdf

[111] "Summary of the HIPAA Security Rule." *Health Information Protection*. Health and Human Services, 25 Apr 2011. http://www.hhs.gov/ocr/privacy/hipaa/understanding/srsummary.html

[112] McBride, Michael.

[113] "Transportation," Kyland. 2009. http://www.kyland.cn/applilist_818.html

Cyber Assets and Functions (Aviation)

The function of the aviation industry is to quickly transport people and materials over long distances in the United States and abroad. The modern aviation industry relies primarily on cyber assets like the air traffic control grid and communication systems like the National Airspace System (NAS), computers, and radar systems (ground and air based). One industry professional also noted that a major asset to the daily operations is a steady and reliable supply of electricity.[114]

The air traffic control grid is a network of regional *centers* that are in constant communication with one another. This allows the air traffic controllers to be aware of aircraft entering their and leaving their airspace at all times.[115,116] Other communication networks include the National Airspace System (NAS), which allows the Federal Aviation Administration (FAA) to monitor facilities, systems, airspace, and routes for air navigation services.[117] They also allow the Transportation Security Administration (TSA) to communicate security advisories directly to the public.[118] Computers are used primarily within airports by airlines to process tickets, reservation, baggage, and passengers.[119] Radar systems help the air traffic controllers to monitor the flight path of inbound and outbound flights. The aforementioned equipment also assists in approach and separation control as aircraft take off and land.

One aviation expert stressed that all of these cyber assets necessitate a large demand for electricity. Electricity powers the systems which measure fuel for aircraft, control the locks on doors leading to the tarmac, etc. While larger airports have a greater demand for electricity, they rely on the same basic assets as smaller airports.

Geography

Assets of the aviation industry are countrywide. The larger airports and nodes of transportation are located in or near major metropolitan areas. The smaller facilities and assets tend to be located in rural areas. The cyber assets that allow airports to perform their functions of approach control and communication are located within each individual airport. This would tend to mitigate the consequences of an attack on one airport's cyber assets because other airports could still function, albeit likely with delays, interruptions in service, and an influx of passengers from the closed airport's region. In this instance, geography would not play a large part in consequence mitigation, but the separate nature of airport communications would prevent major industry collapse.

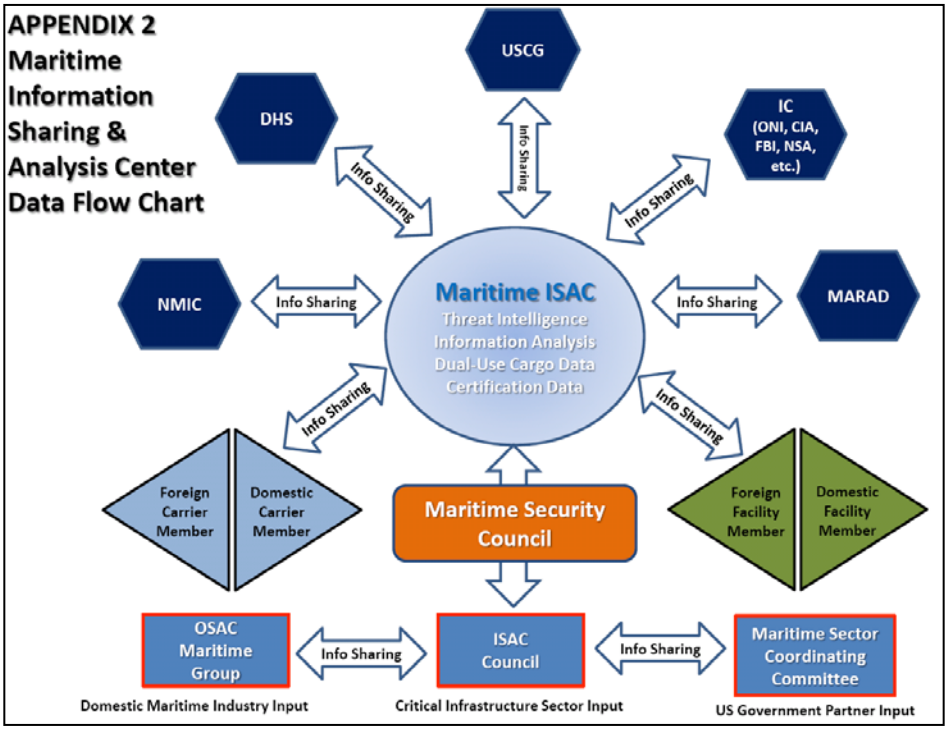
---

[114] Interview with a senior aviation official at Easterwood Airport, College Station, TX. 17 February 2011.
[115] Interview with a senior aviation official at Easterwood Airport, College Station, TX. 17 February 2011.
[116] "Flight Delay Information - Air Traffic Control System Command Center." *Flight Delay Information - Air Traffic Control System Command Center*. 05 Mar. 2011. http://www.fly.faa.gov/flyfaa/usmap.jsp
[117] United States of America. Department of Homeland Security. Office of Infrastructure Protection. *National Infrastructure Protection Plan (NIPP) Sector Specific Plan (SSP): Transportation Systems*. DHS, May 2007. 20 Feb. 2011. http://www.dhs.gov/xlibrary/assets/nipp-ssp-transportation.pdf
[118] United States of America. Department of Homeland Security. Office of Infrastructure Protection. *National Infrastructure Protection Plan (NIPP) Sector Specific Plan (SSP): Transportation Systems*. DHS, May 2007. 20 Feb. 2011. http://www.dhs.gov/xlibrary/assets/nipp-ssp-transportation.pdf
[119] Interview with a senior aviation official at Easterwood Airport, College Station, TX. 17 February 2011.

Cyber Assets and Functions (Maritime Transportation)

Aside from electronic navigation equipment on board ships, enterprise management software and communications networks and systems associated with the Maritime Information and Analysis Center (M-ISAC) and the HomePort information sharing system are the primary cyber assets of the maritime mode of transportation.

M-ISAC was formed in 2003 "to serve as the focal point for gathering and disseminating information regarding maritime threats to interested stakeholders."[120] The purpose of M-ISAC is to provide a forum for sharing threat and vulnerability information between various government agencies with maritime interests. M-ISAC is coordinated by the U.S. Coast Guard's Office of Port and Facility Activity.[121]



Organization chart of M-ISAC

HomePort is the communications system by which the maritime community communicates to the public and shares information on maritime dangers. It also serves as the U.S. Coast Guard's primary tool to "support the sharing, collection, and dissemination of Sensitive But Unclassified

[120] United States of America. Department of Homeland Security. Office of Infrastructure Protection. *National Infrastructure Protection Plan (NIPP) Sector Specific Plan (SSP): Transportation Systems*. DHS, May 2007. 20 Feb. 2011. http://www.dhs.gov/xlibrary/assets/nipp-ssp-transportation.pdf

[121] Thomason, Ronald. "Role of the Maritime ISAC: Training, Drills, Exercises, and Resource Allocation." Small Vessel Security Threat Conference. Ronald W. Shane Center, Miami Beach, FL. 8-9 Feb. 2011. Lecture.

(SBU) information, including Sensitive Security Information (SSI), For Official Use Only (FOUO), and Law Enforcement Sensitive (LES)."[122]

According to the TSA, other maritime-related cyber assets include electronic data interchange systems which alert the Customs Service about suspicious cargo and vessels of interest (VOI), electric navigation equipment on ships, and mechanisms to publish marine casualty reports.[123]

Geography

Assets of the maritime transportation industry are, perhaps obviously, located in bodies of water. Similar to the aviation industry, the maritime industry's cyber assets enjoy a degree of separateness from one another. For instance, ports of entry are located around the coastline of the United States. A disruption in the cyber assets of a west coast port will have little effect on the cyber assets and operations of an east coast port.

Cyber Assets and Functions (Mass Transit)

Mass transit includes heavy rail (subway systems), bus systems, and light rail (commuter trains). Aside from electrical components on board buses, subway trains, and commuter trains, SCADA systems are used to control track direction and railroad signals. The mass transit industry also uses a robust information sharing network.[124] Components of this network include the Mass Transit Resource Center (MTRC) and the Public Transit Information Sharing and Analysis Center (PT-ISAC).

According to DHS, MRTC "provides a comprehensive database for the mass transit industry to access information on a broad spectrum of subjects pertaining to mass transit security, including material not readily available in a consolidated format elsewhere."[125] It is also used by the TSA to "provide timely security alerts, advisories, and information bulletins to mass transit and passenger rail agencies."[126]

The Public Transit Information Sharing and Analysis Center (PT-ISAC) is the primary communication system for sharing threat information between relevant entities in charge of

[122] United States of America. Department of Homeland Security. Office of Infrastructure Protection. *National Infrastructure Protection Plan (NIPP) Sector Specific Plan (SSP): Transportation Systems*. DHS, May 2007. 20 Feb. 2011. http://www.dhs.gov/xlibrary/assets/nipp-ssp-transportation.pdf
[123] "Maritime Transportation Security Act of 2002," H.R. 107-295, 107th Cong. (2002) (enacted). Text available at: http://www.tsa.gov/assets/pdf/MTSA.pdf
[124] http://www.masstransitmag.com/publication/article.jsp?pubId=1&id=918&pageNum=3
[125] United States of America. Department of Homeland Security. Office of Infrastructure Protection. *National Infrastructure Protection Plan (NIPP) Sector Specific Plan (SSP): Transportation Systems*. DHS, May 2007. 20 Feb. 2011. http://www.dhs.gov/xlibrary/assets/nipp-ssp-transportation.pdf
[126] United States of America. Department of Homeland Security. Office of Infrastructure Protection. *National Infrastructure Protection Plan (NIPP) Sector Specific Plan (SSP): Transportation Systems*. DHS, May 2007. 20 Feb. 2011. http://www.dhs.gov/xlibrary/assets/nipp-ssp-transportation.pdf

providing security for their respective transit systems. Currently, over 400 public transit systems are included in PT-ISAC.[127]

Geography

Unlike aviation and maritime assets, the operations of the mass transit industry tend to cluster in major population centers. This is understandable; between commuter trains, subways, and bus systems, densely populated urban areas have larger demands for public transportation services on a daily basis. In the event of an attack, the mass transit industry of a city could have a disproportionate percentage of its assets at risk, compared with aviation or maritime assets.

Cyber Assets and Functions (Rail)[128]

For the daily operation of trains, automated control systems (including SCADA), information systems, and communications networks are used to control track switches and signals and automate control processes.[129,130] The primary information sharing component of the railway system is the Railway Alert Network (RAN). This network serves as the information hub in which stakeholders can "research, receive, analyze, and transmit security information."[131] According to the NIPP, RAN also "links Federal national security and military personnel, and major customer associations with the freight railroads on a 24 hours per day, 7 days per week (24/7) basis."[132] RAN is operated by the Association of American Railroads (AAR) Operations Center. Also associated with RAN is the Surface Transportation Information and Analysis Center (ST-ISAC) which "collects, analyzes, and disseminates information on physical and cyber threats [to the railway mode of transportation]."[133]

Geography

The rail industry is unique within the Transportation sector because it uses SCADA systems to perform its functions. In turn, while the physical assets (i.e. railroads and trains) may

---

[127] United States of America. Department of Homeland Security. Office of Infrastructure Protection. *National Infrastructure Protection Plan (NIPP) Sector Specific Plan (SSP): Transportation Systems*. DHS, May 2007. 20 Feb. 2011. http://www.dhs.gov/xlibrary/assets/nipp-ssp-transportation.pdf

[128] "Trains" and "rail" refer only to freight and cargo trains since subways and commuter trains are included in the Mass Transit section.

[129] Bates, Theunis. "Scores Killed in Indian Train Crash." *AOL News*. 19 July 2010. 5 Mar. 2011. http://www.aolnews.com/2010/07/19/scores-killed-in-indian-train-crash-sabotage-probed/

[130] United States of America. Department of Homeland Security. Office of Intelligence and Analysis/Directorate for Preparedness. *(U//FOUO) Strategic Sector Assessment: The Terrorist Threat to the U.S. Commercial Passenger and Freight Rail System*. Homeland Infrastructure Threat and Risk Analysis Center (HITRAC), 24 May 2006. 5 Mar. 2011. http://abcnews.go.com/images/WNT/terrorist_threat_us_rail_system.pdf

[131] United States of America. Department of Homeland Security. Office of Infrastructure Protection. *National Infrastructure Protection Plan (NIPP) Sector Specific Plan (SSP): Transportation Systems*. DHS, May 2007. 20 Feb. 2011. http://www.dhs.gov/xlibrary/assets/nipp-ssp-transportation.pdf

[132] United States of America. Department of Homeland Security. Office of Infrastructure Protection. *National Infrastructure Protection Plan (NIPP) Sector Specific Plan (SSP): Transportation Systems*. DHS, May 2007. 20 Feb. 2011. http://www.dhs.gov/xlibrary/assets/nipp-ssp-transportation.pdf

[133] United States of America. Department of Homeland Security. Office of Infrastructure Protection. *National Infrastructure Protection Plan (NIPP) Sector Specific Plan (SSP): Transportation Systems*. DHS, May 2007. 20 Feb. 2011. http://www.dhs.gov/xlibrary/assets/nipp-ssp-transportation.pdf

sprawl throughout the country, the factories and depots that employ the SCADA systems may not be as widely disbursed.

Cyber Assets and Functions (Highway)

The function of the highway system is to provide a path by which goods and services reach their markets. While the road systems in urban areas rely on SCADA for the operation of traffic lights and signals, the interstate highway system's dependencies on them are minimal.

Future Trends

Advances in the aviation industry highlight future cyber trends in the transportation sector. The advent of cyber-physical systems (CPS) allows for cyber assets and physical assets to be closely connected, like "smart" infrastructure. In the aviation industry, CPS allow aircraft to monitor their own operating conditions, conduct diagnostic tests in real time and report those conditions to ground control stations. The aircraft can use smart-sensor fabrics and on board networking to accomplish these tasks.[134] This technology would mark a significant step forward in the aviation world because each aircraft could be considered cyber infrastructure.

Water Sector

The water system is run by a series of computer assets, facilities, networks, and equipment referred to as industrial control systems (ICS). They control most of the basic functions administered by a waterworks company. These functions include the monitoring of the water in the source, control of the treatment processes, maintaining the high quality of water, and the delivery of water to the consumer. It also includes managing the treatment and distribution operations and controlling the pressure and flows of water in both water and waste water pipelines. To complete these functions, the system is set up to perform data logging, alarming, and diagnostic functions on the entire network so that the large, complicated process can be effectively overseen and maintained by a centrally located and relatively small staff.

Cyber Assets and Functions

ICS is a general term that encompasses several types of control systems, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and Programmable Logic Controllers (PLC). Each of these individual systems control different parts of the total network however, because they generally work in congruent with each other, the sector generally refers to the ICS as a whole instead of the individual programs listed below.[135]

- SCADA: in networks where data must be collected and controlled by a central location, this highly distributed system can be used to control geographically dispersed assets. For the water sector, this includes the functions involved in water distribution and wastewater collection.

[134] Adam, Nabil. "Workshop on Future Directions in Cyber-Physical Systems Security". *Department of Homeland Security*. January 2010. http://www.ee.washington.edu/faculty/radha/dhs_cps.pdf
[135] United States American Water Works Association. *Roadmap to Secure Control Systems in the Water Sector*. 2008.

- DCS: control systems that oversees the use of multiple, integrated sub-systems responsible for controlling the functions of a specific, local process. This occurs at the water and wastewater treatment processes.

- PLC: computer-based devices which are responsible for controlling the actual industrial equipment and processes.

Geography

Water companies have to control of a system that reaches a very large area. Generally, one company is responsible for the water supplies of an entire municipality. The ISC then has to incorporate the Internet, public telephone, and common wires. The physical and cyber systems are highly connected, allowing for a small amount of staff in a central location to control the entire network. The increasing reliance on cyber assets tends to decrease the ease with which the staff can operate the system manually.[136]

Future Trends

The major security issue with the water sector is the mixture of engineering and construction that could be as old as a century and the ever-increasing demands of modern society. The core of the water pipe system was not built with a computer system in mind.[137] Having to go back and incorporate an extremely complex automated system to the already stressed water works network makes the entire scheme more prone to attacks. Constantly adding additional layers onto the computer system allows for opportunities of unanticipated interactions between the software programs. There have been industry wide recommendations to decrease these vulnerabilities. The most prominent is to design both the physical system and ICS so that the main functions can continue to be performed even after a cyber attack occurs.[138] This would require a mixture of cyber and manual actions to be activated when an attack is detected.

Primary Critical Infrastructure Cyber Assets

While researching the 18 DHS-identified critical infrastructures, three primary critical infrastructure cyber assets were identified: IT and Communications, Enterprise Management Systems, and Industrial Control Systems.

IT and Communications Sector

The IT and Communications sectors are unique in that they comprise the cyber assets that are being examined in relation to all other sectors. Attacks on or failures of these sectors would only be problematic in relation to the other critical infrastructure sectors that rely on information technology for their own functions. For some sectors, the primary security goal with respect to IT is to limit the dependency of the sector on internet connectivity and reduce external access. Where

[136]Adam, Nabil. United States. *Workshop on Future Directions in Cyber-Physical Systems Security*, 2010.
[137]Adam, Nabil.
[138]Adam, Nabil.

external access is required, redundancy and secure authentication are the primary means of defense against external threats. For the purpose of this analysis, the Information Technology and Communications sectors will be analyzed together as they work in conjunction to provide cyber assets to all other sectors.

Most basically, the IT sector can be described as the computing power and software used to manage and process digital data.[139] Computers, servers, and electronic devices make up the hardware part of the IT sector, whereas operating systems and software such as Windows, SCADA systems, and SAP make up the software side. Communications assets refer to the data connections that link together the separate components of the IT sector. Fiber optics cables and routing technology are the primary components of the Communications sector, and it is dominated by a small group of "tier-1" service providers including AT&T, Verizon, and Qwest.[140] Neither the IT sector nor the Communications sector alone can provide what we consider to be "cyber" assets or functions, rather it is the combination of the two which create these capabilities, which is why we address them together here.

Cyber Assets and Functions

In the personal computing space, Windows is the most dominant operating system, with roughly ~90% of the market share, though Apple's OSX is growing rapidly in share. It is difficult to measure the share of the market taken by linux, given that it is freely downloadable and easily installed alongside Windows installations (dual-booting). The number of malicious software threats against Windows-based machines is well-known, though the reasons for this are disputed. Some argue that the inherent nature of the operating system make it an easy target for attack. Microsoft has designed Windows to work easily and transparently with 3rd party software, making it easier for programmers to write code that will alter the system without the user's knowledge. Others argue that the amount of malicious code written for Windows is merely a function of its distribution, meaning that it is simply more profitable to attack the OS with the widest install-base. Threats to OSX have increased in recent years as the popularity of Mac computers grows, lending credibility to this argument.

In the server space, estimates vary on install base. Linux leads in the 60% to 75% range, Windows Server is estimated in the 20% to 35% range, and various Unix operating systems are estimated in the single digits.[141] There is little data on how these server systems are divided by industry served or size of the server. Also, estimates are based only on publicly accessible servers, further clouding the data.

Private Tier 1 service providers make up the top level of internet routing, and would create the greatest disruption of effectively taken offline. Examples of Tier 1 providers include AT&T, Verizon, Qwest, NTT Communications, Level 3, and Global Crossing. A successful attack on such an organization would likely not destroy large amounts of critical data; rather it would interrupt the flow of data through the internet. These service providers do not pay for "peering" with other service providers, which essentially means that they own and control the actual fiber

[139] (Department of Homeland Security 2009)
[140] (van der Berg 2008)
[141] (Q-Success 2011)

and routing equipment that is used to direct data across the internet. Attacks on lower tier service providers would cause some disruption, but damage would be on a much smaller scale and would likely have greater backups and redundancies.[142]

Geography

Geographic distribution of the IT and Communication sectors is wide and constantly evolving. These assets simply follow the populations and IT functions that they serve. Physical data transmission lines typically have the greatest bandwidth in-between major population centers, with smaller branches serving less-populated areas. Hundreds of undersea fiber-optics cables connect the nations of the world, and in most areas these lines of communication are highly redundant. While the breach of a major cable might reduce bandwidth between certain areas, other pathways would remain in operation. Only certain geographically isolated areas, such as small Pacific island chains, remain vulnerable from having only a single line of data transmission to the wider global internet. All non-local internet traffic is resolved through a set of 13 root nameservers spread across the globe. Four of these nameservers are physically located in the United States, with two in Maryland and two in California. The other nine nameservers are not located in individual locations, but are physically dispersed across many geographic locations, allowing for greater security and redundancy. Each dispersed nameserver acts as a singular installation using a technology called "Anycast."[143] Though there have been multiple cyber attacks on the root nameservers, none have been considered successful, and no physical attacks have taken place. A coordinated physical attack would be extremely difficult given the wide geographic dispersion of the physical components that make up these nameservers.[144]

Future trends

Future trends in the IT and Comm sectors are extremely difficult to forecast given the rapid pace of evolution in the industry. In the IT sector, there is a constant arms race of technological development leading the way with security evolving to address new vulnerabilities. Whenever a new technology is implemented, there is a potential for new "zero-day" exploits, or attacks that are undiscovered and unknown by anyone except for the attacker. In communications, bandwidth will continue to grow, as well as redundancies in cable linkages around the world. Countless miles of data cables are laid each day, far exceeding the rate at which these cables are retired. In the future, it will be likely that physical attacks on cyber assets will become increasingly difficult given advances in redundancy and data recovery, yet opportunities for cyber attack using malicious code and deceptive practices will continue to grow as technologies become increasingly complex and transparent to the end user. One promising trend is the continued growth of diverse open source software and operating systems. Though a wider diversity among operating systems will increase the complexity of the cyber eco-system, it reduces the ability of a targeted exploit to spread across multiple machines, and the open-source nature of many of these programs makes detection and repair of vulnerabilities easier. Finally, a trend that cannot be ignored is the increasing use of mobile data.[145] This technology has created a new set of challenges with regard to secure

[142] (Pesante 2008)
[143] (The IETF Trust 2006)
[144] (Marti 2011)
[145] (Marti 2011)

authentication and encryption, given that data is broadcast rather than confined to a physical data cable, however wireless technology is still tightly integrated into the network of physical data transmission lines. Each wireless access point, from WiFi routers to cellular towers, is ultimately connected to the wider internet by a physical data connection.

Enterprise Management Systems

Basics

An Enterprise Management System (EMS) is network management systems designed to manage devices, independent of vendors and protocols, in IP-based enterprise networks.[146] These systems are essentially software suites capable of running every technical aspect of a business. An EMS requires a system administrator to handle the numerous diverse devices utilized.

Another important feature of these systems is that it allows for real-time processing.[147] This is an essential part of any business or organization dealing with inventory, particularly those who use lean manufacturing processes, which is becoming more and more popular.[148]

Known Vulnerabilities

Almost every source on the subject states that the most dangerous vulnerabilities of Enterprise Management Systems are the small, simple weaknesses. According to Alex Rothacker of AppSec's Team SHATTER (Security Heuristics of Application Testing Technology for Enterprise Research), there are ten vulnerabilities that are particularly common.

1. Default, blank, and weak username/password
2. SQL injections
3. Extensive user and group privileges
4. Unnecessarily enabled database features
5. Broken configuration management
6. Buffer overflows
7. Privilege escalation
8. Denial-of-service attack
9. Unpatched databases
10. Unencrypted sensitive data at rest and in motion[149]

---

[146] Kakadia, Deepak. Enterprise Management Systems Part I: Architecture and Standards. Sun Microsystems, Inc. April 2002.
[147] Staehr, Lorraine. Understanding the role of managerial agency in achieving business benefits from ERP systems.
[148] Lean manufacturing trims waste with ERP/WMS. Modern Materials Handling. 2008. http://web.ebscohost.com.lib-ezproxy.tamu.edu:2048/ehost/pdfviewer/pdfviewer?sid=4e839089-0d59-4b14-af01-94c76c4821f9%40sessionmgr114&vid=2&hid=111
[149] Chickowski, Ericka. The 10 most common database vulnerabilities. SQL Manager.net- EMS Database Management Solutions. http://www.sqlmanager.net/en/articles/1640

Moves in the Industry

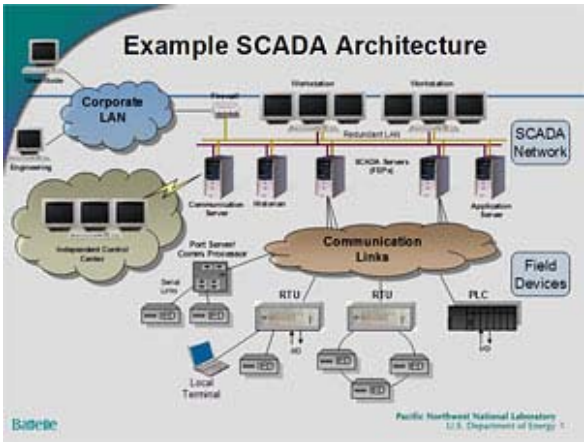
In the last twenty years, there have been three distinct phases of development in the technology of enterprise management systems. The first phase was a transition from a mainframe design to a distributed network architecture. This new design was comprised of several separate local area networks (LANs). The second phase of this evolution was linking all the separate LANs into an enterprise-wide network. The final phase has been the transition of this integrated system into the Web. Additionally, as these systems have become more popular and produced by several different vendors, the need for standardization has arisen.[150]

Industrial Control Systems (ICS): Supervisory Control and Data Acquisition (SCADA) and Distributed Control Systems (DCS)

Overview

Industrial control systems are a fundamental component of most critical infrastructures in the United States, including electric, water, oil/gas, chemicals, pipeline and transportation[151]. Industrial control systems typically fall under two categories: Supervisory Control and Data Acquisition (SCADA) systems and Distributed Control Systems (DCS).

Supervisor Control and Data Acquisition (SCADA) systems are a type of Industrial Control Systems that are made up of two main components: the control center and the plant that it controls.[152] The control system (also known as the master terminal unit or MTU) is the nucleus of a SCADA system and is composed of human machine interfaces (HMI), engineering workstations, plant data information, databases and other components. The control network can then be connected to both on-site and remote site remote terminal units (RTUs) by radio and satellite links, telephone lines and Internet connections. An example of a SCADA system is shown, with external connections to corporate networks:[153]



Distributed Control Systems (DCS) are mainly used for controlling industrial processes but are typically contained in a single geographic region or plant, unlike SCADA systems which have

[150] Kakadia, Deepak. Enterprise Management Systems Part I: Architecture and Standards. Sun Microsystems, Inc. April 2002.
[151] "Architecture for Secure SCADA and Distributed Control System Networks." Juniper Networks, 2010. Web. 20 Apr 2011. http://www.juniper.net/us/en/local/pdf/whitepapers/2000276-en.pdf
[152] Chandia, Rodrigo, et al. "Security Strategies for SCADA Networks." *Critical Infrastructure Protection.* New York: Springer, 2008.
[153] United States. Cyber Security: Protecting Our Nation's Critical Infrastructure 2006. Web. 12 Apr 2011. http://eioc.pnnl.gov/research/cybersecurity.stm

long-range communication capabilities.[154] Therefore, communication between DCS elements is done using local area network (LAN) capabilities. However, DCS and SCADA systems are often used in conjunction with each other and the vulnerabilities and trends affecting one system will normally affect the other. Therefore, for the purposes of this section, the term ICS will not separate between the two systems.

Known Vulnerabilities

While ICS systems have been in use for years and are prevalent throughout the world, there have only been a few recorded cases of deliberate attacks on ICS systems.[155] However, ICS systems have multiple known vulnerabilities that may become exploited in the upcoming years:

- External connectivity: SCADA systems are becoming increasingly connected and remotely accessible to corporate networks and the Internet:
- Commodity software and hardware solutions: Many ICS systems employ Windows computers or software and TC/IP networking; thus passing on their vulnerabilities
- Computer controlled controllers: Computer and operating systems are replacing human control and greatly increasing system complexity.
- Rapidly growing global workforce: The ability to exploit ICS vulnerabilities is rapidly becoming more common.
- Open design: The information necessary to exploit these systems may be readily available
- Increasing size and functionality: ICS are increasingly taking on new roles which may open them up to new access points

Moves in the Industry

Many of the vulnerabilities in the above section are a result of the recent trends in the ICS community. These trends can typically fall under three categories:

1. Increased Connectivity: SCADA systems are increasingly connected to Internet connections and business or corporate networks.[156] Additionally, remote connections are being added to allow for access from separated locations.
2. Increased Complexity: ICS systems are being used in most, if not all, of the critical infrastructures in the United States.[157] Also, new components and networks are being added that increase interdependency.
3. Commercial, off-the-shelf (COTS) software: ICS are employing components that are made up of or use COTS software which increases the amount of information available about the software.

---

[154] Stouffer, Keith, Joe Falco, and Karen Scarfone. United States. Guide to Industrial Control Systems (ICS) Security. 2008. 20 Apr 2011. http://csrc.nist.gov/publications/drafts/800-82/draft_sp800-82-fpd.pdf
[155] Tsang, Rose. "Cyberthreats, Vulnerabilities and Attacks on SCADA Networks." Retrieved 20 Apr 2011. http://gspp.berkeley.edu/iths/Tsang_SCADA%20Attacks.pdf
[156] "Understanding SCADA System Security Vulnerabilities." Riptech, 01 2001. Web. 20 Apr 2011. http://www.iwar.org.uk/cip/resources/utilities/SCADAWhitepaperfinal1.pdf
[157] Robles, Rosslin. "Vulnerabilities in SCADA and Critical Infrastructure Systems." International Journal of Future Generation Communication and Networking 99-104. Web. 20 Apr 2011. http://www.sersc.org/journals/IJFGCN/vol1_no1/papers/14.pdf

Literature Review

The increased digitization of the modern world has prompted widespread discussion among academics, subject matter experts and industry officials concerning cyber-security in critical infrastructure. These experts have suggested countless methodologies to address a diverse number of issues in this field. The following literature review examines the international literature on cyber-security assessments as well as sector specific studies and methods for analyzing interconnectedness between sectors. Our methodology contributes to the literature by providing a holistic criticality assessment for cyber assets.

Critical Infrastructure and Cyber Security Across the World

The problems associated with cyber security and critical infrastructure are not unique to the United States. As information technology and communications continue to rapidly develop, countries across the world must also safeguard against the dangers their increasingly connected critical infrastructure will face. To gain a greater understanding of worldwide efforts to battle cyber vulnerabilities, we identify the critical infrastructure protection policies of 25 countries: Algeria, Australia, Austria, Brazil, Canada, Estonia, Finland, France, Germany, Hungary, India, Italy, Japan, Korea, Malaysia, the Netherlands, Norway, New Zealand, Poland, Russia, Singapore, Spain, Sweden, Switzerland, and the United Kingdom.[158]

The following sections outline some of the patterns in the worldwide mission to protect critical infrastructures as well as some regional or state anomalies in basic approaches to critical infrastructure identification and cyber security.

Defining "Critical Infrastructure"

Across the international sphere, definitions of what constitutes a "critical infrastructure" varied in terms of specificity and subject matter. Many countries, such as Brazil, Finland, Korea, and Russia, do not even have a clear definition outlining the country's identification of "critical infrastructures," or other variants of the term. At the other end of the spectrum, countries such as Germany, Norway, Switzerland, and the United Kingdom have fairly comprehensive and specific definitions. In between, some of the countries used broad, sweeping terms to outline what makes a sector or entity "critical" in comparison to others. For full critical infrastructure definitions from each country, see Appendix: "Country Critical Infrastructure Definitions."

In general, most definitions contained several common elements concerning what form a critical infrastructure may take (See Table 1). The most common concerns "physical structures" (facilities, sites, installations, constructions, etc) followed closely by "information technology" (logical systems, virtual networks, communication networks, etc). Some definitions also addressed services, typically in the form of government, public, and emergency services. Out of the fourteen countries, only three specifically noted the nature of critical infrastructures being "interconnected" entities.

[158] These countries are included on the basis of access to English-translated government documents outlining critical infrastructure protection as well as the existence of public policy concerning critical infrastructure protection.

Table 1				
Countries	**"Form" Elements in Critical Infrastructure Definitions[159]**			
	Physical	Information Technology	Services	Interconnected
Algeria	X	X		
Australia	X	X		
Austria	X	X	X	
Canada	X	X	X	X
Estonia	X		X	
Germany	X			
Hungary	X	X	X	X
Japan	X		X	
The Netherlands	X			
Norway	X			
New Zealand	X	X		
Spain	X	X		
Switzerland	X	X	X	X
United Kingdom	X	X	X	

In addition, the definitions also contained similarities regarding the impact or consequences of degradation or loss of entities classified as "critical infrastructures" within their country (See Table 2). All fourteen identified the "economy" (economic wellbeing, economy operation and activities, etc) as an impact factor when identifying infrastructures as critical. All but Australia noted the criticality of public health and safety impacts, and all but four addressed national or public security impacts. Definitions addressing impact on state institutions for governance as well as social factors such as lowered public confidence were less common.

Table 2					
Countries	**"Impact" Elements in Critical Infrastructure Definitions**				
	(National) Security	Public Health/Safety	Economy	State Institutions	Social Factors
Algeria	X	X	X		
Australia	X		X		X
Austria		X	X	X	
Canada	X	X	X	X	
Estonia		X	X		X
Germany	X	X	X		X
Hungary	X	X	X		
Japan			X		X

The Netherlands	X	X	X	X	
Norway	X	X	X	X	
New Zealand	X	X	X		
Spain	X	X	X	X	
Switzerland	X	X	X	X	X
United Kingdom		X	X		X

Despite the commonalities between country definitions, some anomalies did exist. Particularly, Hungary, the Netherlands, Norway, and Switzerland mentioned impact to the environment or ecology as a defining element. Also, very few gave a specific scope of the impacts. Only Canada specified the potential for different impact scopes, stating that debiliation or destruction of critical infrastructure could have effects "within and across provinces, territories, and national borders."[160]

Critical Infrastructure Identification

Though not all the countries' studied had a definition or justification for identifying infrastructures that are critical, most did have a list specifying sectors, structures, and services deemed critical to the country's mission and objectives. Like the definitions, however, the lists varied from country to country (See Table 3). For a complete list of critical infrastructures in each country, see Appendix "Country-Critical Infrastrutures Definitions."

Table 3

Countries	Energy/Power	Transportation	Communications	Banking/Finance	Government Services	Water	Health	Food	Manufacturing/ Industries	Emergency Services
Algeria	X	X	X	X	X		X	X		X
Australia	X	X	X	X		X	X	X		
Austria	X	X	X		X	X				
Brazil	X	X	X	X		X	X			
Canada	X	X	X	X	X	X	X	X	X	
Estonia	X	X	X	X			X	X		
Finland	X	X		X	X	X	X	X	X	X
France	X	X	X	X	X	X	X	X	X	
Germany	X	X	X	X	X	X	X	X	X	X
Hungary	X	X	X	X	X	X	X	X	X	
India	X	X	X	X						X
Italy	X	X	X	X	X	X	X	X		X
Japan	X	X	X	X	X	X	X			
Republic of	X	X	X	X	X					X

[160] Canada. "National Strategy for Critical Infrastructure," 2009: 2.

Korea										
Malaysia	X	X	X	X	X	X	X		X	X
The Netherlands	X	X	X	X	X	X	X	X	X	
New Zealand	X	X	X	X	X					X
Norway	X	X	X	X	X	X	X	X		X
Poland	X	X	X	X	X	X			X	X
Russia			X	X	X					
Singapore	X	X	X	X		X	X	X		
Spain	X	X	X	X	X	X	X		X	
Sweden			X	X		X				
United Kingdom	X	X	X	X	X	X	X	X		X

Critical Infrastructure Cyber Security

The Swiss Federal Institute of Technology Center for Strategic Studies in Zurich published the International CIIP Handbook in 2009, which did a comprehensive study on 25 national critical information infrastructure protection policies. Throughout their analysis, they found that cyber security policies for critical infrastructure were at "various stages of implementation," with differing focuses on information security, counterterrorism, as well as ensuring the effective operation of critical infrastructures.[161] In terms of public-private partnerships in combating cyber security threats, Switzerland, the Republic of Korea, and the UK were shown to have "strong links" between the business community and the government, whereas others still appear to be struggling to balance "security requirements and business efficiency."[162] To combat cyber security threats to critical infrastructure, many countries have adopted Computer Emergency Response Teams (CERTs),[163] and an increasing reliane on "e-Governance" has also led many countries to adopt more comprehensive cyber security measures.[164]

In terms of how critical infrastructure issues are perceived in policy and political rhetoric, the study found that four perspectives dominate, with one usually trumping the others: a national-security perspective, a law enforcement perspective, an economic perspective, and an IT-security perspective.[165] For example, after the Madrid bombings in 2004, the European Council released "Critical Infrastructure Protection in the Fight Against Terrorism," instilling a framework in many

[161] Center for Security Studies. *International CIIP Handbook 2008/2009: An Inventory of 25 National and 7 International Critical Information Infrastructure Protection Policies*. Ed. Elgin M. Brunner and Manuel Suter. Zurich: Swiss Federal Institute of Technology: 534.
[162] Ibid 535.
[163] Countries with national CERTs include: Australia, Austria, Argentina, Belgium, Brazil, Brunei, Cambodia, Canada, Chile, China, Croatia, Denmark, Estonia, Finland, Germany, Hungary, Israel, Japan, Latvia, Lithuania, Luxembourg, Malaysia, Mauritius, Myanmar, The Netherlands, New Zealand, Norway, Oman, Philippines, Poland, Qatar, Saudi Arabia, Singapore, Slovakia, Slovenia, South Korea, Spain, Sweden, Switzerland, Taiwan, Thailand, Tunisia, Turkey, Ukraine, United Arab Emirates, United Kingdom,United States, Uruguay, Vietnam. Compiled from "National Computer Security Incident Response Teams." *Software Engineering Institute*. Carnegie Mellon, 17 Febr 2010. 23 Apr 2011. http://www.cert.org/csirts/national/contact.html; "Member Teams." *About FIRST*. Forum of Incident Response and Security Teams, 23 Apr 2011. http://www.first.org/about/organization/teams/
[164] United Nations Educational, Scientific and Cultural Organization. "Country Profiles of E-Governance." Paris: 2002.
[165] Center for Security Studies 536.

European countries focusing on the sociological and psychological impacts regarding critical infrastructure.[166] On the other hand, given its history, Japan focuses on disaster resilience measures to ensure continuity of critical services.[167]

Sector Specific Literature

Before assessing the criticality of different cyber systems, it is useful to observe the current status of industry control systems (ICS) in the literature regarding those systems. For the purposes of this literature review, "ICS" refers to many types of industry control systems, including assets like SCADA, DCS, Enterprise Application Systems (EAS), and Energy Management Systems (EMS). By studying this literature, we can develop a better sense of the areas to which we can add value to the modern discourse. This section will provide a brief overview of existing literature on ICS as it relates to the study of industry standards for process control system security, ICS vulnerabilities, threats to ICS, methodologies proposed by scholars and other authors, basic trends in the ICS discourse, and the future of ICS in scholarly and policy discourse.

Standards

A subset of ICS literature, including publications from Sandia National Lab and Idaho National Lab, delves into the topic of industry standards for industrial control systems. Each national lab has researched and published numerous reports on the importance of maintaining minimum and uniform standards of cyber security of ICS. For instance, Sandia's Center for SCADA Security focuses on research, training, and standards development.[168] Many of the reports by the Center provide in-depth analyses and studies of industry standards as they relate to SCADA/DCS systems.[169,170] Additionally, the Center's SCADA Test Bed program (NSTB) supports development of industry standards as they relate to the uniform implementation of cyber security initiatives by different agencies across the Department of Energy (DOE).[171]

At the same time, Evans, Hill, and Rodriguez (2005) compare and contrast three cross-industry cyber security standards using "Information Technology—Code of Practice for Information Security Management (ISO/IEC 17799)" as their baseline. They examined characteristics of this measure along with "Process Control Securities Requirements Forum (PCSRF) System Protection Profile for Industrial Control Systems (SPP-ICS)," "Security Technologies of Manufacturing and Control Systems (ISA-TR99.00.01-2004)," and "Integrating Electronic Security into the Manufacturing and Control System Environment (ISA-TR99.00.02-

[166] Burgess, J. Peter. "Social Values and Material Threat: the European Programme for Critical Infrastructure Protection." *International Journal of Critical Infrastructure Protection*. 3.3/4 (2007).
[167] Aung, Zaw Zaw and Watanabe, Kenji. "A Framework for Modeling Interdependence in Japan's Critical Infrastructure." *Critical Infrastructure Protection III*. Ed. C. Palmer and S. Shenoi. International Federation for Information Processing, 2009.
[168] "The Center for SCADA Security." *Sandia National Laboratories: Securing a Peaceful and Free World through Technology*. 28 Apr. 2011. http://www.sandia.gov/ccss/
[169] R. E. Carlson, J. E. Dagle, S. A. Shamsuddin, R. P. Evans, *A Summary of Control System Security Standards Activities in the Energy Sector,* DOE Office of Electricity Delivery and Energy Reliability, October 2005.
[170] R. Halbgewachs, *Control Systems Security Standards Accomplishments & Impacts* Tech. Rep. SAND2007-7019, Sandia National Laboratories, November 2007.
[171] "NTSB Fact Sheet." *National SCADA Test Bed*. Idaho National Laboratory. 28 Apr. 2011. http://www.inl.gov/scada/factsheets/d/nstb.pdf

2004).[172] This helps security experts in the field of ICS to "identify the similarities and differences between standards, which can contribute to selecting the best security practices and help strengthen sections of the standards in future revisions."[173]

Evans agrees in his 2006 work "Process Control System Cyber Security Standards – An Overview", where he outlines various industry standards for process control systems. He asserts that security standards are a crucial element of systems and cyber-security personnel would be wise to study the trends and effectiveness of each policy before choosing one to implement for their own ICS.[174]

We conclude that many different authors have thoroughly covered the topic of industry standards of ICS.

ICS vulnerabilities

Many different scholars, subject matter experts (SMEs), industry groups, and government agencies have studied the basic components, uses, and vulnerabilities of SCADA. In fact, as Ralston, Graham, Heib (2007) note, there are many offices and divisions in the federal government that are dedicated specifically to assessing risk posed by SCADA systems.[175] The contemporary literature on this topic seems to focus predominantly on vulnerability and threat assessment, rather than consequences.

Ralston, et al (2007) mention that within DHS, the National Infrastructure Advisory Council (NIAC) convergence work group "is investigating the cyber security of SCADA and process control systems…"[176] The National Communication System (NCS), also under DHS, conducts risk assessment on communication systems that make use of SCADA.[177] DHS's National Cyber Security Division (NCSD) includes the Control Systems Security Program (CSSP), which "leads an initiative to secure our nation's critical infrastructure by identifying, analyzing, reducing cyber risks associated with control systems that govern our infrastructures."[178] Finally, U.S. Computer Emergency Response Teams (CERTs) have also completed extensive studies on the vulnerabilities of SCADA.[179]

---

[172] Evans, Robert P. "A Comparison of Cross-Sector Cyber Security Standards." Idaho National Laboratory Publication. Sep. 2005. http://www.inl.gov/technicalpublications/Documents/3395027.pdf

[173] Evans, Robert P. "A Comparison of Cross-Sector Cyber Security Standards." Idaho National Laboratory Publication. Sep. 2005. http://www.inl.gov/technicalpublications/Documents/3395027.pdf

[174] Evans, Robert P. "Process Control System Cyber Security Standards – An Overview." Idaho National Laboratory Publication. May. 2006

[175] Ralston, P.A.S., J.H. Graham, J.L. Heib. "Cyber Security Risk Assessment for SCADA and DCS Networks." ISA Transactions. 10 Jul. 2007.

[176] Ralston, P.A.S., J.H. Graham, J.L. Heib. "Cyber Security Risk Assessment for SCADA and DCS Networks." ISA Transactions. 10 Jul. 2007.

[177] *NCS | National Communications System*. 28 Apr. 2011. http://www.ncs.gov/index.html

[178] US-CERT (United States Computer Emergency Readiness Team) Control System Documents. US-CERT, 2006. http://www.us-cert.gov/control_systems/csdocuments.html

[179] Nelson, Trent. "Control System Security Center Common Control System Vulnerability." Idaho National Laboatory and the Department of Homeland Security. Nov. 2005. http://www.us-cert.gov/control_systems/pdf/csvul1105.pdf

Most of the literature on ICS concerns vulnerabilities. What's more, there is a general consensus among authors that vulnerabilities facing ICS are increasing. Robles and Choi (2009) indicate that the increased networkedness of ICS with COTS technology with known vulnerabilities and weaknesses increases the vulnerabilities of the ICS systems themselves.

While Shea (2003) and Robles and Choi (2009) also provide in-depth discussions on ICS vulnerabilities,[180] Permann and Rohde (2005) provide more technical methods on how to actually mitigate those vulnerabilities.[181] They expound on open source vulnerability assessment methods like Nmap, Nessus, STAT Scanners (for Windows products), Ethereal, Ettercap, Metaspoloit, Debuggers, Fuzzers, and Subject Matter Experts (SMEs).[182]

Fink, Spencer, and Wells (2006) conduct a vulnerability assessment on different ICS like SCADA, energy management systems, process control systems, and their components.[183] In addition, the author(s) conveniently categorize ICS vulnerabilities into: clear text communications, account management, weak/no authentication procedures, coding practices, unused services, network addressing, scripting and interfacing ,programming, unpatched components, web servers and clients, perimeter protection, and enumeration.[184]

Fabro and Nelson (2007) also contribute to the discourse of ICS vulnerability mitigation. They advocate a technique commonly found in physical protection systems called "defense-in-depth," where refers to having layered security measures and increasing redundancy at critical vulnerability points. Specifically, Fabro and Nelson (2007) indentify areas in which defense-in-depth could and should be applied, including "maintenance of various field devices, telemetry collection, and/or industrial-level process systems, access to facilities via remote data link or modem, public-facing services for customer or corporate operations, a robust business environment that requires connections among the control system domain, the external Internet, and other peer organizations."[185] The authors also provide recommendations to ICS vendors on how to mitigate vulnerabilities.

Private industry groups have published an abundance of material relating to ICS vulnerability within their respective sectors. Examples of report-publishing groups are the Instrumentation, Systems, and Automation Society (ISA),[186] the National Institute for Science and Technology (NIST), the Chemical Sector Cyber Security Program—organized by Chemical Info

[180] Cogwell "Critical Infrastructures" - Chp4 –by Dana A. Shea
[181] Permann, May Robin and KennethRohde. "Cyber Assessment Methods for SCADA Security." Idaho National Laboratory Publication. Jun. 2005.
[182] Permann, May Robin and KennethRohde. "Cyber Assessment Methods for SCADA Security." Idaho National Laboratory Publication. Jun. 2005.
[183] Fink, Raymond K., David F. Spencer, Rita A. Wells. "Lessons Learned From Cyber Security Assessments of SCADA and Energy Management Systems." Idaho National Laboratory Publication. Oct. 2006.
[184] Fink, Raymond K., David F. Spencer, Rita A. Wells. "Lessons Learned From Cyber Security Assessments of SCADA and Energy Management Systems." Idaho National Laboratory Publication. Oct. 2006.
[185] Fabro, Mark and Trent Nelson. "Control Systems Cyber Security: Defense-In Depth Strategies." Idaho National Laboratory Publication. Oct. 2007.
[186] Tieghi, Enzo M. "Integrating Electronic Security into the Control Systems Environment: differences IT vs. Control Systems." http://www.isticom.it/documenti/evidenza/13_Enzo_M_Tieghi.pdf

Tech Council (ChemITC), the International Electrotechnical Commission (IEC), the American Gas Association (AGA), and the North American Electrical Reliability Council (NERC).[187]

Threats to ICS

But uniform operating standards also have a downside. As Robles and Choi (2009) argue, the unclassified nature of uniform security standards makes it much easier for potential attackers to gain knowledge about how the security systems for ICS actually work.[188]

Much literature, including portions of Cordesman (2002) focuses on cyber threats like Russia, China, and Iran. He and other authors site figures such as "DOD detects 80-100 potential hacking incidents a day" and often assert that the Russian and Chinese governments may support these attempts.[189] Cordesman (2002) and Gewirtz (2009) discuss the desire of non-state actors acquiring the capabilities to conduct cyber attacks on U.S. critical infrastructure. In particular, Gewirtz (2009) asserts that increased interconnectedness of various networks and technologies also increases the chance that a single terrorist with Internet access could bring down the entire U.S. power grid. Both authors devote attention to discussions of insider threats—a potential theft or sabotage attack from within one's own government or organization.[190,191]

The United States Computer Emergency Readiness Team's (US CERT) Control Systems Security Program (CSSP) has developed a list of the cyber threats facing U.S. critical infrastructure.[192] This includes in-depth analysis of motivations and capabilities of a wide spectrum of potential adversaries. On this list are *entities* like national governments, terrorists, industrial spies and organized crime groups, hacktivists, and hackers.[193] The list is also broken down into specific cyber threat techniques to include bot-network operations, malicious activity from foreign intelligence services and criminal groups, phishing and spamming attacks, spyware/malware authors, and terrorist operations.[194]

In addition, Robles and Choi (2009) provide a discussion of the potential avenues of action that could be taken by an attacker, should they get access to an ICS. The list includes the

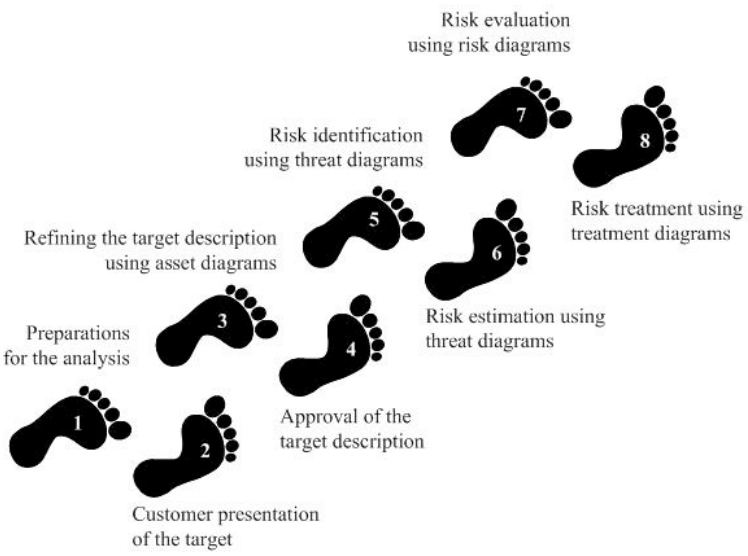
[187] "(Revised) Implementation Plan for Cyber Security Standards CIP-002-1 through CIP-009-1." North American Electric Reliability Council. http://www.nerc.com/fileUploads/File/Standards/Revised_Implementation_Plan_CIP-002-009.pdf
[188] Robles, Rosslin John and Min-kyu Choi. "Assessment of Vulnerabilities of SCADA, Control Systems and Critical Infrastructure Systems." International Journal of Grid and Distributed Computing. Vol. 2, No. 2. Jun. 2009.
[189] Cordesman, Anthony H., and Justin G. Cordesman. *Cyber-threats, Information Warfare, and Critical Infrastructure Protection: Defending the U.S. Homeland*. Westport, CT: Praeger, 2002.
[190] Gewirtz, David. "How Critical Infrastructure is at Risk of a Cyber Attack." Journal of Counterterrorism and Homeland Security International Summer 2009.
[191] Cordesman, Anthony H., and Justin G. Cordesman. *Cyber-threats, Information Warfare, and Critical Infrastructure Protection: Defending the U.S. Homeland*. Westport, CT: Praeger, 2002.
[192] "US-CERT: Control Systems - Cyber Threat Source Descriptions." *US-CERT: United States Computer Emergency Readiness Team*. 29 Apr. 2011. http://www.us-cert.gov/control_systems/csthreats.html
[193] "US-CERT: Control Systems - Cyber Threat Source Descriptions." *US-CERT: United States Computer Emergency Readiness Team*. 29 Apr. 2011. http://www.us-cert.gov/control_systems/csthreats.html
[194] "US-CERT: Control Systems - Cyber Threat Source Descriptions." *US-CERT: United States Computer Emergency Readiness Team*. 29 Apr. 2011. http://www.us-cert.gov/control_systems/csthreats.html

disruption of various processes, equipment and property damage, the compromise of integrity of status and display screens, or the takeover of a physical control station.[195]

Regarding information sharing about threats, DHS has worked with private industry to establish Information Sharing and Analysis Centers (ISACs).[196] The purpose of ISACs is to "advance the physical and cyber security of the critical infrastructures of North America by establishing and maintaining a framework for valuable interaction between and among the ISACs and with government."[197] ISACs are used in different sectors of critical infrastructure, including across the transportation sector (see *Transportation Sector* for diagram), energy sector, water sector, healthcare sector, and so on. Additionally, stakeholders have developed a Multi-State ISAC (MS-ISAC) primarily to serve as **"**the focal point for cyber threat prevention, protection, response and recovery for the nation's state, local, territorial and tribal (SLTT) governments.**"**[198]

While we have a solid understanding of the potential threats to our cyber networks, the basic trend of increasing connectivity of ICS to outside networks and increasing interactions with COTS systems increases the attractiveness of ICS targets to potential attackers.

Methodologies



In addition to thorough study of the threats to and vulnerabilities of cyber assets, there are many different methodologies that shed light on designed to assess different portions of the risk analysis equation for ICS. For example, in the OCTAVE method developed by the CERT at Carnegie Mellon University and used by DOD and UK Ministry of Defense CERTs, the user inputs data for an operationally critical threat, asset, and vulnerability evaluation.[199]

By contrast, Aagedal, den Braber, Dimitrakos, Gran, Raptis, and Stolen (2002) developed the eight-step CORAS method (pictured below).[200] This solution offers few quantitative results, yet it clearly explains the steps that need to be taken in risk management assessment in the realm of cyber security.

[195] Robles, Rosslin John and Min-kyu Choi. "Assessment of Vulnerabilities of SCADA, Control Systems and Critical Infrastructure Systems." International Journal of Grid and Distributed Computing. Vol. 2, No. 2. Jun. 2009.
[196] "National Council of ISACs." *ISAC Council*. http://www.isaccouncil.org/
[197] "National Council of ISACs." *ISAC Council*. http://www.isaccouncil.org/
[198] *Multi-State Information Sharing and Analysis Center (MS-ISAC)*. 28 Apr. 2011. http://www.msisac.org/
[199] "OCTAVE Information." *Security Risk Solutions, Inc.* 28 Apr. 2011. http://www.securityrisksolutions.com/OCTAVE.htm
[200] *The CORAS Method*. 29 Apr. 2011. http://coras.sourceforge.net/

Haimes and Chittester (2005) use interoperability input-output modeling (IIM) in an attempt to quantify consequences of cyber attacks on ICS, including SCADA.[201] Their metrics are "economic inoperability measured in dollars lost for each interdependent sector of the economy, and functional inoperability measured in each [CI] sector's percentage of dysfunctionality."[202]

DiBiasi (2007) also puts forth a methodology for analyzing the impact of cyber threats. Criticality, recovery, effect, vulnerability, and shock value are included as the primary factors of his CREVS methodology to ultimately justify allocation of resources. The user determines a qualitative result for each indicator and is given a numeric score. These numbers are totaled to determine if it is necessary to allocate more resources to protect against a particular threat.[203]

Trends

Gone are the days in which ICS operate on their own networks, isolated from computer networks across the country. With ever-increasing interconnectedness across the board between and within industries, SCADA systems are now more connected to common networks like Ethernet, wireless networks, shared lease lines, the Internet, and other COTS.[204] This leads to increased functionality of the systems and, perhaps, a higher level of convenience for the system's users. However, a 2004 GAO report asserts that the increased incorporation and adoption of standardized technology with known vulnerabilities increases vulnerabilities to the ICS itself.[205] In turn, potential attackers with knowledge of how to exploit vulnerabilities of the more common COTS systems can also access data controlled by SCADA systems.

Future of ICS discourse

As mentioned, the existing literature on SCADA systems is disproportionately oriented toward threats to SCADA security and established and increasing vulnerabilities facing the systems. The future of research in this regard, at least in the immediate term, seems to indicate similar trends. On May 25-26, 2011 industry experts and *one* DHS official will meet in San Francisco, CA for a conference entitled "Strategies and Technical Solutions for Economically

---

[201] Haimes, Yacov Y., and Clyde G. Chittester. "A Roadmap for Quantifying the Efficacy of Risk Management of Information Security and Interdependent SCADA Systems." *Journal of Homeland Security and Emergency Management* 2.2 (2005). https://www.webdepot.umontreal.ca/Usagers/langlost/MonDepotPublic/infrastructures/Risk%20SCADA%20Systems.pdf

[202] Haimes, Yacov Y., and Clyde G. Chittester. "A Roadmap for Quantifying the Efficacy of Risk Management of Information Security and Interdependent SCADA Systems." *Journal of Homeland Security and Emergency Management* 2.2 (2005). https://www.webdepot.umontreal.ca/Usagers/langlost/MonDepotPublic/infrastructures/Risk%20SCADA%20Systems.pdf

[203] DiBiasi, Jeffery R. "Cyberterrorism: Cyber Prevention vs. Cyber Recovery." Naval Postgraduate School Thesis Dec. 2007.

[204] *Making the Nation Safer: the Role of Science and Technology in Countering Terrorism*. Washington, D.C.: National Academy, 2002.

[205] United States. Government Accountability Office. Critical Infrastructure Protection. *Challenges and Efforts to Secure Control Systems*. 2004.

Managing Risk in a Multi-Threat Environment."[206] The two day conference will feature sessions like "Gaining Clarity On The Current And Evolving Multi Threat Environment And Quantifying Risk In Terms Of Financial Value," "Understanding How The SCADA Network Interacts With The Corporate Network To Gain A Better Understanding Of What Measures Must Be Implemented To Effectively Separate These Networks To Improve Your Security," and "Implementing User Awareness And Training Your Work Force To Mitigate Accidental Insider Threats," among other topics.[207] This single conference may not be indicative of comprehensive future SCADA/ICS, but it is evident that discussion remains centered on threat identification and vulnerability mitigation. In turn, there will likely remain a dearth of literature and commentary on what the ramifications would be if these systems were disabled or compromised.

Interdependence and Cascading Effects

Modern infrastructure consists of highly interconnected and digitized networks, both within and between sectors. None of the sectors identified as "critical" by the Department of Homeland Security exists in isolation of the others. Rinaldi (2004) asserts that without an understanding of the interaction and interdependencies between and within infrastructure, the validity of any analysis regarding these issues would be limited and the policy recommendations stemming from the conclusions could result in imprudent decisions during a crisis. Thus, engineers and policy makers alike have studied the interconnectedness of critical infrastructure and the consequences of one sector's failure on other sectors. Yet interconnectedness in critical infrastructure is a relatively young field of study that needs further development. In this section, we examine the patterns in the research of interconnectedness, particularly the problems associated with a lack of metrics and acknowledgement of cascading effects in criticality assessments.

According to Rinaldi (2004) and confirmed by Ralston, Graham, and Patel (2006) and Theoharidou, Kotzanikolaou, and Gritzalis (2010), the literature concerning interdependence falls into six broad categories: (1) Aggregate supply and demand tools, (2) Dynamic simulations, (3) Agent-based models, (4) physics-based models, (5) population mobility models, and (6) Leontief input-output models. Here, we examine other trends in the literature and discuss input-output methodologies in detail.

Since many of these interdependencies arise from overlapping and connected cyber components, many articles address industrial control systems such as SCADA and DS, or IT and communications systems. Most methodologies attempt to model interdependencies using both quantitative and qualitative approaches, yet few offer a solution to the "metrics problem." Most authors focus on the vulnerability of assets due to interconnectedness rather than criticality. Only a handful of articles discuss methodologies for determining criticality based on interdependencies in networks. Despite the plethora of papers on interconnectedness and cascading effects, the study of interdependency in critical infrastructure is still relatively young and requires further research to fully understand the nature of these complex networks.

[206] Proc. of Strategies & Technical Solutions for Economically Managing Risk in a Multi-Threat Environment, San Francisco, CA. 28 Apr. 2011. http://www.managing-scada-security-risks.com/4/agenda/23/agenda/
[207] Proc. of Strategies & Technical Solutions for Economically Managing Risk in a Multi-Threat Environment, San Francisco, CA. 28 Apr. 2011. http://www.managing-scada-security-risks.com/4/agenda/23/agenda/

Haimes (2005) nicely summarizes the importance of studying interdependences in critical infrastructure to homeland security. Each network is internally interdependent (for instance, the electricity grid requires the integrity of other parts of the grid to function) and externally dependent (the electricity industry depends on telecommunications for production and distribution of power). These interdependencies are inherently complex, multi-faceted and difficult to model. Yet the vulnerabilities stemming from this connectedness necessitates detailed and holistic methodologies to model interdependencies and the consequences of cascading failures across networks. Haimes also points out that despite the numerous papers on the subject, there is limited knowledge about the risk, interconnectedness and complexity of interdependent critical infrastructure.

A commonly used methodology to address this daunting task is the input-output inoperability model (IIM). Based on the theory of market equilibrium by economist Wassily Leontif, the IIM has been applied to quantitatively model the interdependencies of complex networks in critical infrastructure. For instance, Chen, Scown, Matthews, Garrett, and Hendrickson (2009) use input-output models to analyze interdependencies in critical infrastructure for large upstream dependencies in the second and third orders of supply chain.

Most IIM methodologies apply financial data as the primary parameter for measuring interdependencies. Macaulay (2008) uses financial data to assess the dependency of one sector on another. By using a dataset based on quantitative and qualitative factors, Macaulay contributes a metrics-based methodology to understand cascading impacts of disruptions in one sector on another.

Yet as Setola, De Porcellinis, and Sforna (2008) point out, financial data can limit the researcher because it provides only one dimension of critical infrastructure, thus reducing the reliability of IIM results. They contend that the IIM model can produce realistic results using a more "fuzzy" data set of based on sector-specific experts in addition to financial data.

Other researchers have applied a probabilistic framework to analyze interdependencies and cascading failures across infrastructure networks. Interdependency research based on probability is typically used as a part of overall risk assessments. Over a series of papers, Dobson, Carreras, and Newman (2003, 2004) present a method for simulating the consequences of the failure of one system on another based on probability. The authors applied the probabilistic model CASCADE to model the interacting infrastructure systems with detail. However, since these papers have only applied CASCADE to the electrical power grid, the model may not be as useful as IIM or other methodologies for analyzing other infrastructure sectors.

Utne, Hoksad and Vatn (2010) also present a probabilistic model for modeling and analyzing infrastructure interdependencies as part of a cross-sector risk and vulnerability analysis. Their user-friendly model identifies independencies by following an initiating event and the consequences. The researcher uses an event tree diagram and traces the cascading effects of the triggering event based on the probability of each event. Though this method can be applied to any infrastructure sector, the model is clunky and is based on vague assessments of likelihood. As such, it is an unreliable method lacking the metrics necessary to determine interdependencies.

Of all the literature on interdependencies in critical infrastructure networks, only a very small portion concerns criticality. Since infrastructure assets (particularly cyber assets) are highly interdependent, the lack of criticality assessments based on cascading effects and interdependency is a major hole in the literature.

Ayyub, Mcgill and Kaminskiy (2007) address the issue of criticality and interdependency in one portion of their holistic approach to critical infrastructure protection. They use a simple technique to identify the economic losses resulting from the loss of an interdependent asset. Large economic losses determine the criticality of a particular asset. Since this is only a small part of their overall portfolio assessment, their approach to determine criticality is overly simplistic and needs to be expanded.

Franchina, Carbonelli, Gratta, Petricca, and Perucchini (2009) develop a global approach for determining criticality based on interdependency, cascading effects and interestingly, Maslow's hierarchy of needs. First, the authors classify resources on a 5 level scale based on Maslow's hierarchy of needs. For example, food, water, energy, health and the environment are all "level 1" critical needs, while finance, culture, icons and meeting places and less necessary human needs are placed on "level 3". The production, transportation, distribution and use of resources that fulfill these needs rely on critical infrastructure. The authors then present a very simple method for modeling cascading effects and dependencies on critical infrastructure using matrices. However, their methodology is also too simplistic and fails to effectively and systematically trace the dependencies of critical infrastructures on one another. Furthermore, their value-based assessment of criticality lacks metrics. This methodology fails to effectively determine criticality of critical infrastructure assets by incorporating interdependency and cascading effects.

Theoharidou, Kotzanikolaou, and Gritzalis (2010) offer the most holistic contribution to the literature on the use of interdependencies in critical infrastructure to determine criticality. The authors also provide a useful definition of interdependencies between sectors. Their methodology applies previous risk and security assessments performed in individual organizations to a sector and intra-sector criticality assessment. In doing so, they distinguish between three different layers of security assessments and create a system for tracing independencies between those layers. By identifying the interfaces between the operator layer, the sector layer and the intra-sector layer, the authors add a new element for determining criticality of assets for infrastructure. Their method is useful for both physical and cyber components of critical infrastructure.

Researchers are just beginning to address the complexity of interdependency in critical infrastructure. Nascent methodologies can be further developed, particularly for criticality assessments. The perennial issue of limited metrics must also be addressed, but a solution to this problem remains elusive. As engineers and policy makers develop sophisticated ways to model interdependencies and cascading effects, policy makers will have better tools to protect our critical infrastructure and preserve our national security, economic security and public safety.

Value-Added of Our Methodology

In the midst of contemporary cyber security discourse, it is necessary to clarify the areas in which our original methodology adds value. Our methodology accomplishes this task in three ways. First, our methodology produces interval level data so that users can clearly measure potential impact areas (national security, economic security, and public safety) vis-à-vis one another. Second, its flexibility allows the end user to adjust its specificity to perform the consequence analysis at the sector level (i.e. prioritizing sectors within the system) or, if necessary or desired, perform the analysis at the asset level (i.e. prioritizing assets within a sector). Third, the format of the methodology mitigates the influence of exaggerated value judgments commonly associated with the practice of assessing the criticality of one's own assets.

Metrics in this sort of analysis are often vague terms. Systems that show "high," "medium," or "low" impact are not particularly helpful when trying to determine consequences. Our original algorithm uses a unique weighting system to produce interval level data so that end users can easily compare impacts on national security, economic security, and public safety. This will allow end users to *see* the areas in which a particular sector of critical infrastructure will have the greatest consequence. Given the current budgetary uncertainties in the federal government, prioritization of resources is more important than ever. We believe our methodology can assist decision makers in that regard.

The methodology's flexible, user-friendly approach allows for the easy adjustment of scope, if necessary or required by the policymaker. For instance, it can be used to prioritize among the 18 sectors of critical infrastructure for the broad purpose of resource allocation at the federal level. On the other hand, it can also be used within sectors to prioritize particular assets for internal resource allocation.

From start to finish, our methodology was developed with the end user in mind. If the end user happens to be a policymaker or someone without specialized industry knowledge, it still allows them to clearly examine the relevance of a piece of cyber infrastructure to our indicators of national security, economic security, and public safety. If the end user is one with specialized industry knowledge, our methodology challenges them to justify their decisions by explaining *how* a particular cyber asset contributes to the functions of each particular indicator that they claim it does. It is not uncommon for industry officials and sector insiders to exaggerate the importance of their own assets to justify resource allocation. To honestly consider prioritization of critical cyber infrastructure, we determined was necessary to remove such biases, to the extent possible. The methodology forces the user to assess whether a particular cyber asset are relevant to the essential functions of national security, economic security, or public safety before making the determination (or not) about the criticality of that asset.

Ideally, the end user of our methodology is not an individual policymaker or SME. Conversely, the methodology was developed to be used by a group of SMEs in conjunction with a policymaker or a representative from a resource-distributing authority. That way, the SMEs can fill out the methodology while answering and clarifying any points for the resource-dispensing agent. In the end, both the SMEs and the individual(s) without specialized industry knowledge should have an understanding of the prioritization of the assets in question and an understanding of the potential consequences, should an asset be disabled.

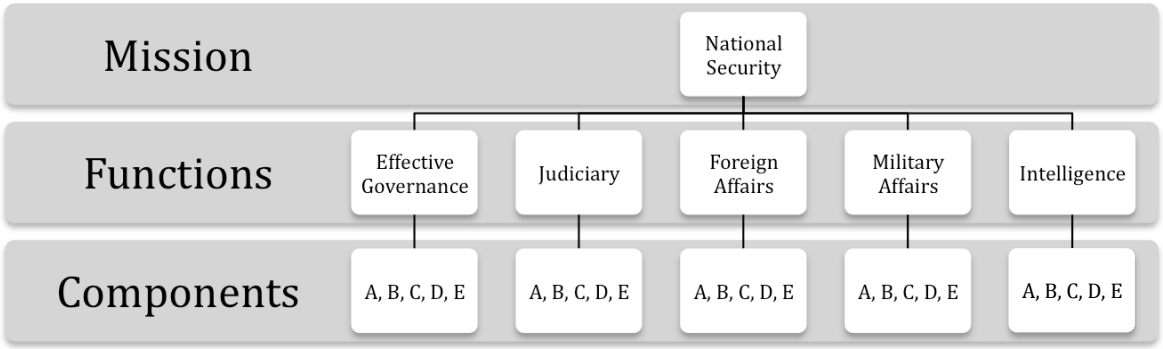
Methodology

Basic Methodology Outline

To gain a comprehensive criticality measurement that reflects the complexity of critical infrastructures, we have devised a methodology that focuses upon the *severity*, *scope*, and *time* impacts on the key critical missions of national security, economic security, and public safety. We have devised a questionnaire, weighting system, and scoring method to compare the severity, scope, and time impacts of different critical infrastructure cyber assets on the three key missions (For the full questionnaire, see Appendix). The methodology requires the user to list the infrastructures or entities he or she needs to prioritize and then answer the questionnaire for each one. This format was chosen for the following reasons:

- *Consistency*: To have a methodology whose goal is prioritization, the method used to study each infrastructure or asset must remain constant for all elements studied. The questionnaire is a consistent structure with a standardized weighting and scoring system.
- *Simplification*: Critical infrastructure has become increasingly complex and interdependent as it relies more and more on cyber assets. The questionnaire methodology breaks down broad missions and forces the user to evaluate which components of the critical infrastructure apply to those broad missions (See Figure ***). It allows the user not only to identify applicable components, but it also prompts him or her to differentiate the various impact levels possible for the critical infrastructure cyber assets.
- *Potential for Expansion*: The questionnaire developed for this project represents a baseline dissection of the DHS's primary concerns of national security, economic security, and public safety. The questionnaire may be expanded depending upon the end user and new developments in cyber security and critical infrastructure with further breakdowns of functions or components and new dependent variables (For expansion suggestions, see Appendix)

Figure 1



Terminology

Mission refers to the three overall components of welfare that would be negatively affected by a disruption or destruction of critical infrastructure. These three *missions* are national security, public safety and economic security. Each *mission* is made of certain ***functions***. These *functions* pertain to the purpose of each mission. For instance, the *functions* of public security are: 1) disease outbreak and mitigation, 2) timely emergency services, 3) state/local law enforcement response, 4) access to basic needs. Certain ***components*** of critical infrastructure are necessary to fulfill those functions.

Severity refers to the extent to which the key missions of national security, economic security, and public safety will be debilitated by a loss of critical infrastructure cyber assets. Once the user identifies the applicable components through the *severity* questions, he or she must estimate the appropriate ***scope*** impacts of each, or how much of the population is adversely affected and how. Next, the user identifies the projected ***time*** impacts of each component. This refers to the cyber asset's recovery time and the duration of primary consequences/effects. The methodology recognizes that the loss of different components result in different impacts, and therefore the user must estimate *scope* and *time* for each component to allow for a comprehensive analysis.

Severity, Scope, and Time Scoring

Severity

When measuring criticality under the measures of national security, economic security, and public safety, one must identify which key components of each actually depend upon the critical infrastructure cyber assets. For the purposes of weighting and time efficiency, we limited the number of components to 5 per function.

In judging severity, one must remember that the loss of some components may be more debilitating than others. In recognizing this fact, however, how does one prevent *every* component from being considered important, and therefore making every entity highly critical? To solve this problem, we utilized the concept and reality of limited resources. For each function, we allowed only 2 out of 5 of the components to be assigned a higher weight (a weight of 3), whereas the other 3 retained a score of 1. We believe that the 2/5 rule for assigning higher weights forces/challenges the user to prioritize using the following considerations:

1. Existing national, state, or local policies and prioritizations.
2. Logical assumptions of dependency, as components may depend upon a single component for functionality or initiation
3. Emphases within the specific sector
4. Limitations of resource allocation

Using these considerations, we assigned weights to each of the components according to the 2/5 rule (See Table 4).

Table 4			
Mission	**Functions**	**Components**	**Weight**
National Security *The protection, maintenance, and resilience of the federal government's ability to ensure effective governance; maintain an effective judiciary; conduct foreign affairs; conduct military operations; collect, analyze, and disseminate all-source intelligence in a timely fashion.*	Effective Governance	General populace giving feedback to government	1
		Holding of elections	1
		Tallying and computing results of elections	1
		Communication of policy, laws, or intentions to wider populace	3
		Communication between local, federal, state, and national levels of government	3
	Judiciary	Maintaining the integrity of evidence for civil cases	3
		Maintaining integrity of evidence for criminal cases	3
		Enabling the trying of cases within courtroom	1
		Maintaining integrity of legal documentation	1
		Communication between trial, appellate, state supreme, and supreme courts	1
	Foreign Affairs	Communication of diplomatic instructions to tasked government personnel abroad	1
		Communication with foreign government representatives on international policy	3
		Deployment of diplomatic personnel to other areas	1
		Security of diplomatic personnel abroad	1
		Secure transportation of the President or high-level government officials overseas	3
	Military Affairs	Transportation of military personnel to and within operational areas abroad	3
		Communication between operational elements and command	3
		Procurement of needed weapons and resources	1
		Military response to national states of emergency	1
		Coordination and communication between military and allies	1
	Intelligence	Tasking of needed intelligence	1
		Intelligence collection (HUMINT, SIGINT, IMINT, etc)	3
		Intelligence processing (decoding, translation, etc)	1
		Intelligence analysis	1
		Intelligence dissemination to appropriate parties	3
Economic Security *Ensuring the security, flow and integrity of monetary and financial data and the control systems that manage the flow of goods*	Security of monetary and financial services	Preventing removal of funds from companies by non-authorized individuals	3
		Preventing access to personal data by non-authorized individuals	3
		Preventing access to address/phone numbers/SSNs/insurance numbers by non-authorized individuals.	1

and services through interstate and international trade.		Preventing access to financial statements and/or company data by unauthorized users	1
		Preventing access to data relating to exchanges and stock markets by unauthorized users.	1
	Flow of monetary and financial services	Maintaining functionality of credit card and electronic systems	3
		Enabling customers to deposit and/or withdraw funds	3
		Enabling banks to transfer funds between each other	1
		Preventing runs on banks	1
		Preventing the value of the dollar from being artificially impacted compared to other currencies	1
	Integrity of monetary and financial services	Preventing monetary and financial data from being destroyed	3
		Ensuring the accuracy of banks' records of holdings	3
		Ensuring individuals' personal information is not maliciously altered	1
		Ensuring banks' customer data is not altered	1
		Maintaining accuracy of data relating to exchanges and stock markets	1
	Flow of goods and services through inter-state trade	Functionality of oil and gas pipelines	1
		Preventing the malicious disruption of supply chain management systems	1
		Preventing the disruption of sea transportation	3
		Preventing the disruption of land transportation	1
		Preventing the disruption of air transportation	3
	Flow of goods and services through international trade	Functionality of oil and gas pipelines	3
		Preventing the malicious disruption of supply chain management systems	1
		Preventing the disruption of sea transportation	1
		Preventing the disruption of land transportation	3
		Preventing the disruption of air transportation	1
Public Safety *The preservation, maintenance, and resiliency of a state/local governments' ability to prevent and mitigate disease outbreak, ensure timely response of emergency services, ensure an effective law enforcement presence, and provide access to basic*	Disease outbreak prevention and mitigation	Dissemination of necessary medicinal supplies among the population.	3
		Identifying and, if needed, quarantining infected individuals	1
		Communication of necessary preventative measures to general public	3
		Communication of general population with public health authorities	1
		Ensuring access to patient records	1
	Emergency services	Notification of an incident to emergency responders	3
		Access of emergency responders to affected area	3

needs for its area of jurisdiction.		Access adequate supplies and equipment for emergency responders	1
		Transportation by emergency responders cannot of victims	1
		Communication between emergency responder elements	1
	Law enforcement	Communication and assessment of alerts from general population of criminal activity	3
		Communication between law enforcement elements	1
		Access to affected area	3
		Physically apprehension of perpetrators	1
		Incarceration of perpetrators	1
	Basic needs	General population access to clean water	3
		General population having shelter against adverse weather	1
		General population access to a safe air supply	3
		General population protection from adverse radiological or chemical elements	1
		General population protection from unsafe structures or environments that threaten physical harm	1

To determine severity, the user must answer a flow of questions as outlined in the example below:

As outlined in the definitions, the infrastructure sector is integral in the missions of:

- ☐ National Security
- ☐ Economic Security
- ☐ Public Safety

(If National Security was checked)

What key functions of national security do the infrastructure affect/perform?

- ☐ Enables the conduct of military operations
- ☐ Enables the conduct of foreign affairs
- ☐ Enables intelligence cycle
- ☐ Enables the conduct of judiciary bodies
- ☐ Enables effective governance

(If "Enables the conduct of military operations" was checked)

Which of these components of ***the conduct of military operations*** does the infrastructure sector perform?

- ☐ Transportation of military personnel to and within operational areas abroad
- ☐ Communication between operational elements and command
- ☐ Procurement of needed weapons and resources
- ☐ Military response to national states of emergency
- ☐ Coordination and communication between military and allies

The **Severity Score** for national security, economic security, and public safety is then computed using the following equation:

$$SEVERITY = \frac{\sum(Component\ Scores)}{(\#\ of\ \ Functions)}$$

Scope

The scope of impact resulting from a critical infrastructure's disruption or destruction must be considered for an overall criticality measurement. We define *scope* as the number of people affected and the degree to which that population is harmed. The user of our methodology will need to assess the possible impact of a destroyed or disrupted cyber component in a critical infrastructure on a population.

Our methodology is flexible enough to be used on the local, regional, or national level. As such, the possible population affected depends on the policy maker. A local official will estimate a much smaller population of people affected than a state or regional policy maker.

To determine scope, the user must answer the following questions for each *component* of the questionnaire identified to be dependent on the infrastructure's cyber assets:

Should the component be lost due to destruction or manipulation of cyber assets, how many people would experience **loss of life**?

>10,000	1,000 - 10,000	100-1,000	50-100	<50	None

Should the component be lost due to destruction or manipulation of cyber assets, how many people would experience **severe injuries/illness**?

>10,000	1,000 - 10,000	100-1,000	50-100	<50	None

Should the component be lost due to destruction or manipulation of cyber assets, how many people would experience **minor injuries/illness**?

>10,000	1,000 - 10,000	100-1,000	50-100	<50	None

Should the component be lost due to destruction or manipulation of cyber assets, how many people would experience **inconvenience**?

>10,000	1,000 - 10,000	100-1,000	50-100	<50	None

The answers to these questions for each *component* determine the scope score. For each component, scope is scored on a scale (See Table 5):

Table 5						
Impact Factor	**5**	**4**	**3**	**2**	**1**	**0**
Population Affected	>10,000	1,000-10,000	100-1,000	50-100	<50	None
Degree of Harm		Loss of Life	Severe Illness/Injury	Minor Illness/Injury	Inconvenienced	

Each score is then plugged into the following equations to determine impact and scope:

$$IMPACT_{scope} = (Lossof\ Life)(PopulationAffected) + (SevereIllnessorInjury)(PopulationAffected) + (MinorIllnessorInjury)(PopulationAffected) + (Inconvenienced)(PopulationAffected)$$

$$SCOPE_{Unweighted} = \frac{\sum_{Components}(IMPACT_{scope})}{(\#\ of\ Functions)}$$

Though these equations provide a score for *scope*, in their current state, they are not weighted on the same scale as *severity* or *time*. Our methodology weights *severity*, *scope and time* on the same scale. Using natural logs and exponential functions, we have created a mathematically correct formula that weights *severity*, *scope and time* on the same scale.

Severity falls on a possible scale between 0 and 9. Thus, we weight *scope* on a scale of 0 to 9 also:

$$\left(\sum_{Components}(Maximum\ Scope\ Scores)\right)^{X} = 9$$

$$X = \frac{\ln(9)}{\ln\left(\sum_{Components}(Maximum\ Scope\ Scores)\right)}$$

$$X = \frac{\ln(9)}{\ln(Maximum\ Scope\ Score)} = \frac{\ln(9)}{\ln(250)}$$

$$SCOPE_{Weighted} = \left(\sum_{Components} (Scope\ Scores) \right)^{\ln(9)/\ln(250)}$$

Time

The consequence of a disrupted or destroyed cyber component in critical infrastructure depends in large part on the *time* it takes for the asset to recover and return to normal operating capacity and the duration of the effects resulting from disruption. Our methodology uses this variable to account for any redundancies and back-ups in critical infrastructure. A cyber asset that can be "re-booted" within minutes may not be as critical as a cyber asset that takes months or years to become operable again.

The questionnaire asks the user the following questions to measure the *time* variable for each *component*:

What is the estimated recovery time of the cyber assets?

Years Months Days Hours Minutes Seconds

What is the estimated time length of the immediate, primary effects upon [national security, economic security, or public safety]?

Years Months Days Hours Minutes Seconds

Behind the scenes, each answer is scored on a scale (See Table ***):

Table 6

Impact Factor	**5**	**4**	**3**	**2**	**1**	**0**
Recovery of Cyber Asset (Checkbox)	Years	Months	Days	Hours	Minutes	Backup Available
Duration	Years	Months	Days	Hours	Minutes	No effect

of effects (for checkbox)						

The following equations are used to calculate the *time* score and are then weighted on the same scale as *severity* and *scope*.

$$IMPACT_{time} = \sum_{Components} (Asset\ \text{Recov}ery)(\text{Pr}imary\ Eff ects Duration)$$

$$TIME_{Unweighted} = \frac{\sum_{Components} (IMPACT_{time})}{(\#\ of\ Functions)}$$

Though these equations provide a score for *time*, in their current state, they are not weighted on the same scale as *severity* or *scope*. Our methodology weights *severity, scope and time* on the same scale. Using natural logs and exponential functions, we have created a formula that weights *severity, scope and time* on the same scale.

Severity falls on a possible scale between 0 and 9. Thus, we weight *time* on a scale of 0 to 9 also:

$$\left(\sum_{Components} (Maximum\ Time\ Scores) \right)^{X} = 9$$

$$X = \frac{\ln(9)}{\ln\left(\sum_{Components} (Maximum\ Time\ Scores) \right)}$$

$$X = \frac{\ln(9)}{\ln(Maximum\ Time\ Score)} = \frac{\ln(9)}{\ln(125)}$$

$$TIME_{Weighted} = \left(\sum_{Components} (Time\ Scores \right)^{\ln(9)/\ln(125)}$$

Methodology Output

After the user completes the questionnaire for each infrastructure or entity, each is scored according to the following equations (See Table 7).

Table 7

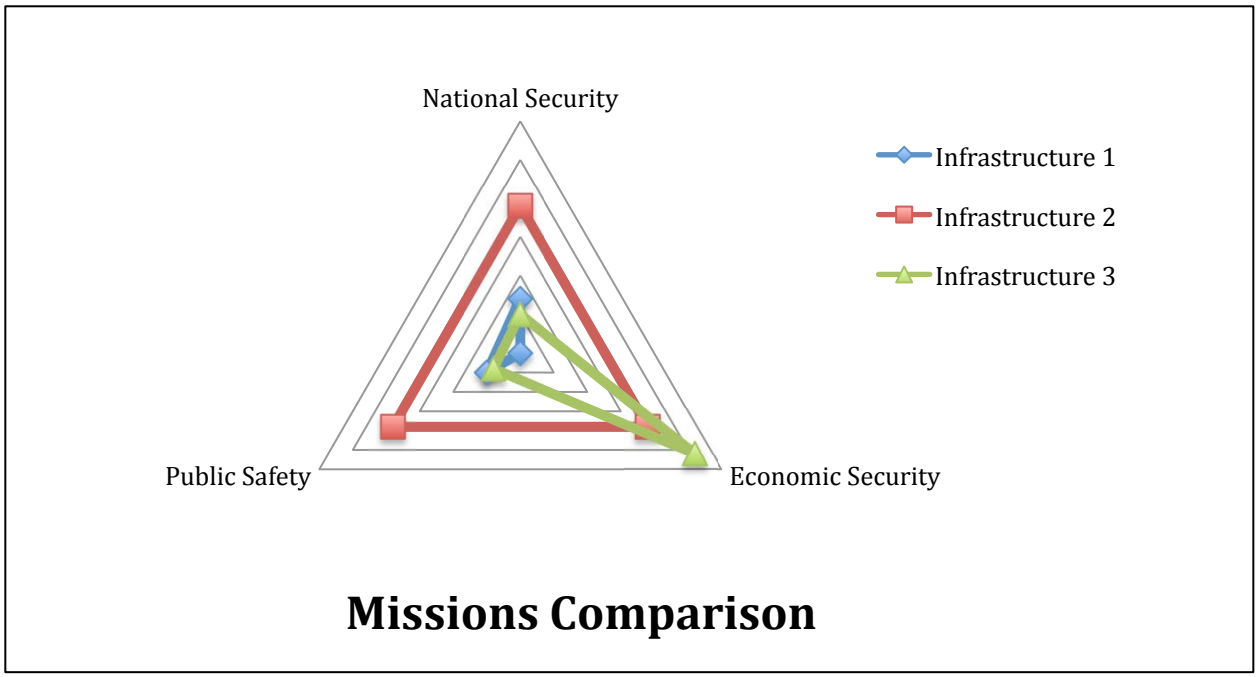
Metric	Equation	Max Score
National Security	$\sum_{\substack{\text{National Security}\\\text{Components}}}(\text{Severity Scores}) + \left(\sum_{\substack{\text{National Security}\\\text{Components}}}(\text{Scope Scores})\right)^{\ln(9)/\ln(250)} + \left(\sum_{\substack{\text{National Security}\\\text{Components}}}(\text{Time Scores}\right)^{\ln(9)/\ln(125)}$	27
Economic Security	$\sum_{\substack{\text{Economic Security}\\\text{Components}}}(\text{Severity Scores}) + \left(\sum_{\substack{\text{Economic Security}\\\text{Components}}}(\text{Scope Scores})\right)^{\ln(9)/\ln(250)} + \left(\sum_{\substack{\text{Economic Security}\\\text{Components}}}(\text{Time Scores}\right)^{\ln(9)/\ln(125)}$	27
Public Safety	$\sum_{\substack{\text{Public Safety}\\\text{Components}}}(\text{Severity Scores}) + \left(\sum_{\substack{\text{Public Safety}\\\text{Components}}}(\text{Scope Scores})\right)^{\ln(9)/\ln(250)} + \left(\sum_{\substack{\text{Public Safety}\\\text{Components}}}(\text{Time Scores}\right)^{\ln(9)/\ln(125)}$	27
Severity	$\sum_{\substack{\text{National Security}\\\text{Components}}}(\text{Severity Scores}) + \sum_{\substack{\text{Economic Security}\\\text{Components}}}(\text{Severity Scores}) + \sum_{\substack{\text{Public Safety}\\\text{Components}}}(\text{Severity Scores})$	27
Scope	$\left(\sum_{\substack{\text{National Security}\\\text{Components}}}(\text{Scope Scores})\right)^{\ln(9)/\ln(250)} + \left(\sum_{\substack{\text{Economic Security}\\\text{Components}}}(\text{Scope Scores})\right)^{\ln(9)/\ln(250)} + \left(\sum_{\substack{\text{Public Safety}\\\text{Components}}}(\text{Scope Scores})\right)^{\ln(9)/\ln(250)}$	27
Time	$\left(\sum_{\substack{\text{National Security}\\\text{Components}}}(\text{Time Scores}\right)^{\ln(9)/\ln(125)} + \left(\sum_{\substack{\text{Economic Security}\\\text{Components}}}(\text{Time Scores}\right)^{\ln(9)/\ln(125)} + \left(\sum_{\substack{\text{Public Safety}\\\text{Components}}}(\text{Time Scores}\right)^{\ln(9)/\ln(125)}$	27

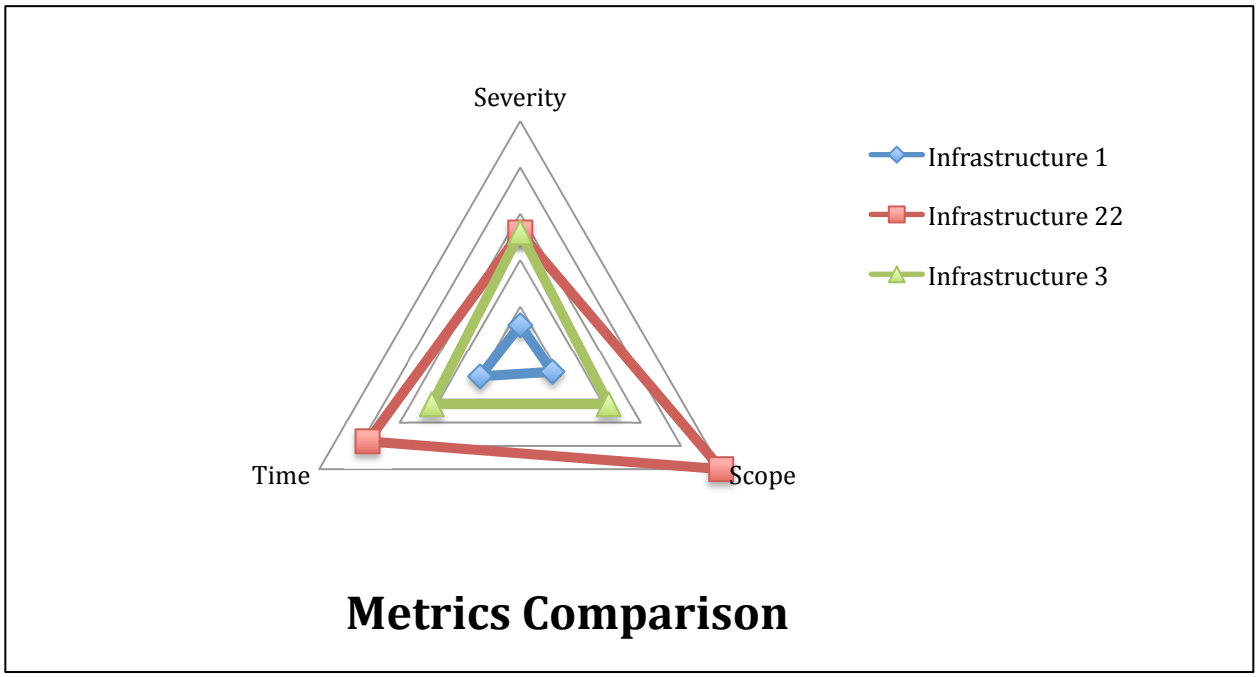
To gain perspective on the comparisons between the infrastructures, the results will be presented in the following formats:

Radar Graph Visual Representation

The final criticality assessments will be presented on a radar graph (see below). This allows the end user to clearly visualize and compare relative consequences on our three missions/indicators vis-à-vis one another. Each layer of the radar graph represents a

different level of criticality. In the example below, Infrastructure 2 has is moderately critical for each mission while Infrastructure 3 is highly critical to the economic security mission and little to no criticality for national security or public safety.





Ratio-Comparison Chart

	Infrastructure 1	Infrastructure 2	Infrastructure 3
National Security	7/27	19/27	26/27
Economic Security	0/27	19/27	5/27
Public Safety	5/27	19/27	4/27
Severity	3/27	19/27	13/27
Scope	4/27	13/27	11/27
Time	5/27	25/27	11/27
Total Criticality	12/82	57/81	35/81

How to Interpret Scores

Since we have designed this methodology to be user friendly, we have formatted the final results to be as easily understandable as possible. Each infrastructure receives a score over the total possible points, or a ratio. A high ratio, or a score close to one, means the infrastructure is more critical.

A policy maker may use the *missions* ratio scores to determine if local, state, or federal agencies should be charged with protecting the cyber assets in each particular infrastructure. For instance, if Infrastructure 1 received ratios of .12, .78, and .45 for national security, economic security and public safety respectively, it may be more prudent for federal agencies to protect cyber components dealing with economic security because this infrastructure is highly critical for this mission.

The results also provide a ratio for metrics. These ratios can also help the policy maker determine which government agencies are necessary to protect and monitor each particular infrastructure. For instance, a high ratio for scope means a federal or state agency would be most effective at protecting the infrastructure. Since the failure of a component in infrastructure would impact a larger population, federal agencies may have greater resources to mitigate such a disaster.

Providing all ratios for the missions and metrics of our methodology in one table allows the policy maker to effectively prioritize infrastructures based on relative criticality. With knowledge of the relative consequences of a cyber failure in critical infrastructure, one can allocate resources more effectively. Furthermore, a policy maker can add additional variables such as costs of protection to determine the relative importance of infrastructure and designate responsibilities among different agencies.

Case Study

We decided that it would be appropriate to test the methodology and to do so we utilized the Texas A&M campus, which is a microcosm of a larger metropolitan area. The campus of Texas A&M hosts a full utilities service, emergency responders, information technology and communications service, a nuclear reactor, and an airport. The utilities sector provides electrical power, water, and sewage for the entire campus that is independent from the utilities for the surrounding municipalities. Emergency responders are also independent, but often work in conjunction with other local emergency responders. The information technology sector is completely independent. Campus-wide routing, connectivity, and hosting is provided by this department, and it controls the sole fiber route by which campus cyber assets are connected to the broader internet. The nuclear reactor is located on university property and is operated by Texas A&M University. Finally, Easterwood Airport is located just west of the Texas A&M campus, and is owned and operated by the university, though it is funded internally.

We identified qualified experts for each sector and conducted personal interviews with each. We walked each expert through the methodology and used their inputs to complete the process for each sector. With each interviewee, we were explicit in our intent to limit the scope of the case study to the actual Texas A&M specific asset, rather than make logical extensions to larger scale operations. For example, our contact at the nuclear reactor provided his thoughts on how the methodology might be completed with regard to a large power generating plant serving a large metropolitan area, but we focused only on the specific research reactor located on campus.

Final scores for each of these sectors were generally low, reflecting the fact that these assets serve a relatively small population, and generally have robust backups in place, both within campus and coming from the surrounding cities of Bryan and College Station. For example, if Texas A&M emergency services are somehow incapacitated, responders can immediately come onto campus from nearby Bryan and College Station facilities.

Table 8[2]

	Airport	Emergency Services	Utilities	Nuclear Reactor	IT
National Security	0	0	0	0	0
Economic Security	3.11	0	6.37	0	8.02
Public Safety	0	5.12	10.61	1.23	0
Total	**3.11**	**5.12**	**16.98**	**1.23**	**8.02**
Severity	0.80	2	8.6	0.75	3.40
Scope	1.08	1.08	4.90	0	1.99
Time	1.24	2.04	3.48	0.48	2.63
Total	**3.11**	**5.12**	**16.98**	**1.23**	**8.02**

[2] To see breakdown of questions answered, please see the compilation of surveys in the Appendix.

Overall Results

Texas A&M University Department of Information Technology

To complete the survey for Information Technology, we interviewed Mr. Willis Marti, who is the Director, Networking and Chief Information Security Officer at Texas A&M University. He is also the Associate Director of the Academy for Advanced Telecommunications and Learning Technologies, and a Senior Lecturer in the Computer Science Department. Mr. Marti has been instrumental in Campus Network improvements, the creation of the Lone Star Education and Research Network (LEARN), and the development of a partnership with the University of Texas to create resilient networking for both schools. In addition, he assisted in the founding of the IT Forum and the IT Advisory Committee. Mr. Marti also initiated the Virtual Network Engineering Laboratory and serves as Co-Principle Investigator for the related NSF grant. He assisted in the development of a successful proposal naming Texas A&M University as a Center of Academic Excellence by the National Security Agency. He also sponsors Texas A&M's nationally recognized Collegiate Cyber Defense Competition (CCDC) Team.

The IT department at Texas A&M uses two server rooms, one located in the Teague building on Main Campus (east of Wellborn Rd.) with the other in the Wehner building on West Campus. There is hosting redundancy between these two server rooms, though off-campus connectivity is routed entirely through the Wehner facility. From there, fiber optic cables run west toward Easterwood airport until they hit a data trunk that runs north the Dallas/Fort Worth as well as south to Houston. Severing this line before it gets to Wehner would eliminate any connection between campus and the wider internet, though the estimate for repair time given a simple cut is measured in hours.

Should critical damage occur on the server rooms themselves, there is secure offsite backup hosted in Dallas, and full contingency plans are in place to restore all missing or corrupted data within 72 hours. Should an outage occur during paycheck disbursal, the plan is to pay employees based on the previous month's earnings, for which there are paper records, and reconcile any differences once the system is back on line. The greatest damage would arise if there is a severe outage in the time immediately preceding graduation. This could result in a delay in degrees being awarded, as grade information would be temporarily unavailable.

For Texas A&M, given the contingency plans in place, the maximum level of damage would be inconvenience, and any problem or primary effect would likely be remedied with a few days.[3]

Easterwood Airport

Easterwood Airport is a small airfield with only two gates that serves the community of Bryan/College Station. It is owned and operated by Texas A&M University. The airport receives

[3] Marti, Willis, interview by George Stasny. *Director, Networking and CISO, Texas A&M University* (April 13, 2011).

between 9 and 12 commercial flights daily from Houston and Dallas, and also accommodates personal aircraft from both domestic and international flights. The current director of Easterwood is John H. Happ, Jr. Mr. Happ has worked at Easterwood Airport since 1996 and was selected as Director of Aviation in 2000, a position he has held ever since. Before moving to the airport, Mr. Happ served as Professor of Aerospace Studies at Texas A&M University. Mr. Happ retired from the United States Air Force in 1996 as a Colonel[4].

All questions on the survey were answered by Mr. Happ during his interview. The vast majority of flights are domestic; however there is the occasional personal international flight. The airport serves 80,000 people yearly, with days surrounding the beginning and ending of University vacations being the busiest, but almost every day has between 100 and 1,000 domestic passengers and less than 50 international passengers. Easterwood Airport only went online during Mr. Happ's tenure, meaning that most manual methods of operations are still readily available. The airport still the paperwork that can be hand-written and faxed to the needed locations, so any inconveniences would be minor and short-lived. All necessary mechanical equipment can also be operated manually[5]. The airport is well insulated from cyber-attacks because of the size of the field and their ability to quickly switch to non-computer based operations. e

Texas A&M University Utilities and Energy Management

This case study was completed with assistance from David Brown, Senior Lead Systems Engineer for Utilities and Energy Management at Texas A&M. We found that the functions performed by this department intrinsically affect a wide variety of other sectors and services, but that backups are robust, and expected down-times from a cyber-attack are minimal.

For National Security, we determined that the utilities department at Texas A&M has almost no impact on any of the functions of national security, however the wider utilities sector as a whole impacts several functions, most notably intelligence collection and effective governance. Economic Security relies very heavily on the utilities sector, both nationally and in our specific case study. Integrity, flow and security of monetary and financial data rely on functional utilities, as do assets concerning trade, such as oil and gas pipelines, and supply chain management systems. Public Safety seems to be the sector most reliant on utilities, especially with our particular case study. Almost all aspects of communication between emergency services depend upon functioning utilities, as well as the general population's access to basic needs such as clean water and air.

For the majority of functions performed by the Utilities and Energy Management Department at Texas A&M, it was determined that reliable backups to cyber assets exist; for

[4] Easterwood Airport. (2011). *Staff*. Retrieved April 27, 2011, from Easterwood Airport: http://www.easterwoodairport.com/staff.html

[5] John H. Happ, J. (2011, April 11). Director of Aviation, Easterwood Airport. (S. Nauss, Interviewer)

example, the largest and most significant buildings on campus all have backup generators. For those functions which are not adequately backed-up, estimates of effect varied based on the type of cyber-attack. For an attack which merely disrupts functionality, the resetting of firmware and rebooting process should have functions restored within minutes. Recovery time is less well-known for cyber-attacks that cause damage to physical components, such as stuxnet-type viruses, as this type of attack has never occurred to the knowledge of our subject-matter expert. These types of concerns raise the criticality estimate for this particular sector.[6]

Texas A&M University Nuclear Science Center

This case was completed with assistance from Dr. William Charlton. Dr. Charlton serves as the Director of the Nuclear Security Science and Policy Institute (NSSPI) and as such directs the overall NSSPI activities. Dr. Charlton is an expert in the area of nuclear nonproliferation research and education. Prior to his appointment at TAMU, he was an Assistant Professor in the Nuclear and Radiation Engineering Program at the University of Texas at Austin from 2000-2003. From 1998-2000, Dr. Charlton was a Technical Staff Member in the Nonproliferation and International Security Division at Los Alamos National Laboratory (LANL). He remains heavily involved with many of the National Laboratories including: consultation on nuclear material safeguards and national security projects, providing graduate and undergraduate students for summer programs and new hires, collaborating with laboratory staff on various funded research projects, and helping to provide continuing education opportunities for laboratory employees. Dr. Charlton's answers on our survey relate to the nuclear research reactor on the Texas A&M campus and not to nuclear facilities in general. He noted that different kinds of nuclear reactors will have different types of consequences if their cyber assets were to be disabled. The primary function of Texas A&M's research reactor is to produce medical isotopes for cancer treatments at hospitals in Houston, TX. For this reason, the consequences, according to Dr. Charlton's answers, relate only to public safety and, more specifically disease outbreak mitigation (check the survey – I'm not sure if he checked another box here). In contrast, Dr. Charlton mentioned that larger nuclear weapons facilities will have a much greater impact on national security than public safety if it were to lose its cyber assets.[7]

Texas A&M Emergency Services

This case study was completed with assistance from Tyler Eschbach, Communications Director for Texas A&M Emergency Services, and examines the Emergency Medical Services (EMS) sector at Texas A&M University and the role of cyber assets in the day-to-day procedures and processes. Through the interview with Mr. Eschbach, and touring of the Texas A&M EMS facilities, it was determined that cyber assets, such as computer call and dispatching software, play an integral role in routine management of emergency dispatches. However, there are

[6] Brown, David, interview by Steph Shaffer. *Senior Lead Systems Engineer for Utilities and Energy Management* (April 20, 2011).

[7] Charlton, William, interview by Matthew and Anderson, Aimee Jennings. *Director of NSSPI* (April 21, 2011).

practical back-ups, overlapping and secondary measures that would allow for adequate service in the event of a cyber asset crash or attack.

Texas A&M University EMS does not support or ensure the adequate working of the functions listed under national security. It is important to note, however, that this case study analyzed the process of the EMS sector under routine circumstances and not under extemporaneous or special conditions.

Also, Texas A&M EMS plays no role in ensuring economic security. As even the billing for completed services is not done by the EMS service, they do not deal with monetary or financial data, nor ensure the flow or trade of goods and services. Therefore, the impact that an attack on the cyber assets would have an economic security is zero.

Finally, Texas A&M Emergency Medical Services' cyber assets do play a substantial role in public safety through the functions of timely emergency services and disease outbreak prevention and mitigation. Under disease outbreak prevention and mitigation, EMS ensures access to patient records and fulfills all components under timely emergency services. Due to the use of computer call receiving, information retrieving, and dispatching, an attack on the cyber assets would have an effect on the integrity of these systems. However, these effects would only have a short-lived impact on the ability of EMS to respond to emergencies and back-ups could take over in a matter of minutes. Therefore, the only impact of a cyber attack on the Texas A&M University would be the inconvenience factor.

Due to the back-ups provided by neighboring cities, the services provided by Texas A&M EMS could be replaced immediately if necessary. Additionally, the functions of the EMS that rely on computer assets could be substituted by non-cyber resources in a matter of minutes. Therefore, the overall impact of a cyber attack would not be substantial and would only have a direct impact for a matter of minutes.[8]

[8] Eschbach, Tyler, interview by Andrew Giblin. *Communications Director for Texas A&M Emergency Services* (April 19, 2011).

Appendix

Country Critical Infrastructure Definitions

Algeria
Algeria's critical infrastructures include physical and information technology facilities which is damaged, destroyed or disrupted would have serious negative effects on several services as security, safety, health and economy for the whole population particularly those in urban sites in Algeria and may affect seriously some countries in Europe.[9]

"The critical infrastructures in Algeria are made up of the following sectors: energy and utilities (electrical power, natural gas and oil transmission systems), communications (telecommunications and broadcasting systems); services (financial services, food distribution and health care); transportation (air, rail, marine and surface); safety (emergency services) and government services (major government facilities and information networks)."[10]

Australia
Those physical facilities, supply, chains, information technologies and communication networks which, if destroyed, degraded or rendered unavailable for an extended period, would significantly impact on the social or economic wellbeing of the nation or affect Australia's ability to conduct national defence and ensure national security.[11]

"Banking & Finance, Communications, Health, Water services, Food chain, Energy, Transport, IT Security"[12]

Austria
"…natural resources; services; information technology facilities; networks; and other assets which, if disrupted or destroyed would have serious impact on the health, safety, or economic wellbeing of the citizens or the effective functioning of the Government."[13]

"In its answer, the Ministry of Internal Affairs clarified that there is a list of civilian objects worthy of protection, but they are not explicitly denoted as critical infrastructure. However, it can be assumed that Critical Infrastructure Protection in Austria manly refers mainly to these objects. The list of civilian objects worthy of protection includes about 180 items, which are categorized in the following classes:

- Institutions of the legislative, executive, and judiciary powers,
- Infrastructure facilities of energy supply companies,

[9] Benouar, Djillali. "Natural Hazards Threats to Critical Infrastructure in Algeria." 1st Annual Conference of the International Society for Integrated Disaster Management. (September 2009): 1.
[10] Ibid.
[11] Commonwealth of Australia. Critical Infrastructure Resilience Strategy. 2010.
[12] Ibid 17.
[13] Brunner, Elgin M., and Manuel Suter. "International CIIP Handbook 2008/2009: An Inventory of 25 National and 7 International Critical Information Infrastructure Protection Policies." Center for Security Studies, ETH Zurich. (2009): 65-66.

• Information and communication Technologies,
• Infrastructure facilities that ensure the provision of vital goods,
• Transport and traffic infrastructures."[14]

Canada
Critical infrastructure refers to processes, systems, facilities, technologies, networks, assets and services essential to the health, safety, security, or economic well-being of Canadians and the effective functioning of government. Critical infrastructure can be stand-alone or interconnected and interdependent within and across provinces, territories, and national borders. Disruptions of critical infrastructure could result in catastrophic loss of life, adverse economic effects, and severe harm to public confidence.[15]

"Energy and utilities, finance, food, transportation, government, information and communication technology, health, water, safety, manufacturing."[16]

Estonia
Vitally important sectors and the ministries administering these are the following:
Maintenance of public order, fire extinguishing and rescue work, organization of protection of data banks – the Ministry of Internal Affairs;
• Functioning of the energy and gas system, organization of supply with staple goods; organization of telecommunications and postal services, and transport – the Ministry of Economic Affairs and Communications;
• Organization of supply with foodstuffs – the Ministry of Agriculture;
• Functioning of the financial system – the Ministry of Finance;
• Organization of health care, social insurance and social welfare, provision of psycho-social help, assistance to refugees and the evacuated, labor force calculation – the Ministry of Social Affairs;
• Organization of protection of cultural property – the Ministry of Culture;
• Organization of environmental protection and monitoring – the Ministry of the Environment.[17]

Finland
Vital functions:
- Strategic Tasks…in securing vital functions
  - Management of government affairs
    - Guaranteeing the proper functioning of the Government
    - National coordination of preparing and handling issues relating to the European Union
    - Functioning of Government communications
    - Maintenance of the situation picture
  - International activity

[14] Ibid 67.
[15] Canada. National Strategy for Critical Infrastructure. 2009: 2.
[16] Ibid.
[17] Brunner and Suter, 117.

        - Maintaining contacts with foreign countries, the institutions of the European Union's bodies and key international actors
        - Protecting and assisting Finnish citizens abroad
        - Securing Finland's foreign trade
        - International military crisis management
        - Civilian crisis management
    - National military defence
        - Preventing and repelling military threats
        - The military situation picture
        - The surveillance and safeguarding of territorial integrity
        - Supporting society and other authorities
    - Internal security
        - Internal security
        - Safeguarding the law enforcement system
        - Public order and security
        - Emergency services and maritime search and rescue
        - Civil defence
        - Flood risk management and dam safety
        - Oil and chemical response at sea
        - Border management
        - Immigration control
        - The management of a major influx of asylum seekers
    - Functioning of the economy and infrastructure
        - The financial system and money management
        - Safeguarding the insurance services
        - Securing the fuel supply
        - Safeguarding the electric power supply
        - Safeguarding the electronic ICT systems
        - Safeguarding the state administration's IT function and information security
        - Supporting the construction and maintenance of warning and alert systems
        - Safeguarding the continuation of transports
        - Safeguarding the primary production of food
        - Safeguarding the water supply
        - Safeguarding food processing and distribution
        - Safeguarding critical industries and services
        - Guaranteeing housing
        - Securing a sufficient labour workforce
        - Maintaining the education and research system
        - Detecting changes in the environment and adapting to them
    - The population's income security and capability to function
        - Income security
        - Social and health care services
        - Guaranteeing the availability of pharmaceuticals as well as medical devices and supplies
        - The detection, surveillance and management system for health risks
    - Psychological crisis tolerance

- Education
- Cultural identity and cultural heritage
- Religious services[18]

France

- Finance,
- Industry,
- Energy,
- The work of the judiciary,
- Public Health,
- The work of national civil authorities,
- Electronic Communication, Audiovisual Media, and Information Technology,
- Transport Systems,
- Water Supply,
- Food,
- Space and Research,
- The Armed Forces.[19]

Germany

Critical infrastructures (CI) are organized and physical structures and facilities of such vital importance to a nation's society and economy that their failure or degradation would result in sustained supply shortages, significant disruption of public safety and security, or other dramatic consequences. [20]

Criticality: A relative measure of the importance of a given infrastructure in terms of the impact of its disruption or functional failure on the security supply, i.e. providing society with important goods and services.[21]

Critical infrastructures

- Transport and traffic
- Aviation, maritime shipping, railways, local traffic, inland waterways transport, roads, postal service
- Highly IT-dependent – control centres, process control technology, supply chain management, traffic management, traffic safety, navigation
- Energy
  - Electricity
  - Nuclear power stations
  - Gas
  - Petroleum
  - Highly IT-dependent – control and regulation of power generation facilities, control and regulation of power transmission facilities, control and regulation of power

[18] Finland, . "The Strategy for Securing the Functions Vital to Society." Security and Defence Committee. (23 Nov 2006).
[19] Brunner and Suter.
[20] Federal Republic of Germany. National Strategy for Critical Infrastructure Protection (CIP Strategy). Federal Ministry of the Interior, 17 June 2009: 4.
[21] Ibid 7.

distribution
- Hazardous materials
  - Chemical and biomaterials
  - Hazardous materials transportation
  - Defence industry
  - Highly critical IT-dependent – control, regulation, monitoring, and distribution of chemicals and biomaterials, monitoring of hazardous materials transportation
- Information technology and telecommunications
  - Telecommunications
  - Information technology
- Finance, monetary system, and insurance
  - Banks, insurance companies, financial service providersm stock exchanges
  - IT-Dependent – secure communications within and between institutions, sub-sector-specific data processing software, cashless payment transactions, interbank transactions, accounting systems
- Supply services
  - Health care
  - Emergency and rescue services
  - Disaster control
  - Food supply
  - Water supply
  - Waste disposal
  - IT-Dependent – command and control centres, communication links, databases, hospital management, databases containing confidential patient records, technical control centres and control systems, medical engineering
- Authorities, administration and justice
  - Government
  - Government agencies
  - Administration
  - Security authorities and organizations
  - Federal armed forces
  - IT-Dependent: fail-safe and confidential communications, specific information systems, databases, control centres/situation and analysis centres
- Other
  - Media and large-scale research institutes
  - Prominent building and cultural assets[22]

Hungary

Interconnected, interactive, and interdependent infrastructure elements, establishments, services, and systems that are vital for the operation of the national economy and public utilities to maintain an acceptable level of security for the nation, individual lives, and private property, as

[22] "Information on critical infrastructures." *Germany Federal Office for Information Security*. Retrieved 6 April 2011. <https://www.bsi.bund.de/ContentBSI/EN/Topics/Criticalinfrastructures/Introduction/Criticalinfrastructure/infocrit.html>.

well as concerning the maintenance of the economy, the public health services, and the environment. [23]

"• Information and Telecommunication Systems,
• Energy,
• Water Supply,
• Transport,
• Public Health,
• Food-Products Supply,
• Banking and Financial Sector,
• Industry,
• Government Institutions,
• Public Security and Homeland Defense.
In addition, a legal definition has been agreed that includes e-communications and postal services among the nation's critical infrastructures."[24]

India
• Banking and Finance,
• Insurance,
• Civil Aviation,
• Telecommunications,
• Atomic Energy,
• Power,
• Ports,
• Railways,
• Space,
• Petroleum and Natural Gas,
• Defense,
• Law Enforcement Agencies.[25]

Italy
• Banking and Finance,
• Public Safety and Order,
• (Tele-) Communication,
• Emergency Services,
• Energy Production, Transportation, and Distribution,
• Public Administration,
• Health Care Systems,
• Transportation and Logistics (Air, Rail, Maritime, Surface),
• Water (Drinking Water, Waste Water Management),

[23] Brunner and Suter, 180.
[24] Ibid 81.
[25] Mishra Vineeta. "Critical sectors to be Y2K ready in time: govt report". In: India Times, 19 October 1999. http://www.apnic.net/mailing-lists/s-asia-it/archive/1999/10/msg00050.html.

• Information Services and the Media,
• Food supply. [26]

Japan
Critical infrastructure" is the basis of people's social lives and economic activities formed by businesses that provide services which are extremely difficult to be substituted by others If its function is suspended, deteriorated or become unavailable, it could have significant impacts on people's social lives and economic activities. [27]

- Data communication
  - Telecommunication services
  - Broadcasting
- Finance
  - Bank
    - Deposit withdrawal
    - Lending
    - Foreign exchange
  - Life insurance
    - Payment of premium
    - Payment of insurance, etc
  - Damage insurance
    - Payment of premium, etc
  - Securities companies
    - Buying and selling of securities, etc.
  - Financial products exchange
    - Mediation of buying/selling of securities, etc. Breakage and representation
    - Breakage of liquidation
    - Establishment of financial products market
- Airlines
  - Passenger and cargo air transportation services
  - Air traffic control service
  - Weather forecast distribution
  - Reservation, ticketing, boarding/cargo procedures
  - Operation and maintenance
  - Flight planning
- Railway
  - Passenger transportation service
  - Ticketing and entrance/exit processes
- Electric Power
  - Public electric power supply industry

[26] Brunner and Suter 213.
[27] Japan. Second Action Plan on Information Security Measures for Critical Infrastructures. 3 Feb 2009: 10.

- Gas
  - General gas business
- The Government and Administrative Services
  - Administrative service of municipal governments
- Medical
  - Medical treatment
    - Acts of medical examination and treatment
    - Record and filing of records
- Water Service
  - Supply of water with water services
- Logistics
  - Transportation and storage of freight[28]

Korea

In Korea, the following sectors are counted among the critical infrastructures that are heavily dependent on information and telecommunication technologies.

• E-Government and National Government Administration,
• National security,
• Emergency / Disaster Recovery Services,
• National Defense,
• Media Service, e.g., Broadcasting Facilities,
• Financial Service,
• Gas and Energy, e.g., Power Plants,
• Transportation, e.g., Subways and Airports,
• Telecommunication.[29]

Malaysia

• Financial Sector,
• Water and Sewerage,
• Communications and Media,
• Energy,
• Health and Emergency Services,
• Industry,
• Central Government,
• Government Services,
• Transportation,
• Military[30]

Norway

[28] Ibid 49-51.
[29] Brunner and Suter 242-243.
[30] Ibid 261.

Critical infrastructures are those constructions and systems that are essential in order to uphold society's critical functions, which in time safeguard society's basic needs and the feeling of safety and security in the general public.
are "merely" very important. Under this method, a product or a service is defined as vital if it "provides an essential contribution to society in maintaining a defined minimum quality level of (1) national and international law and order, (2) public safety, (3) economy, (4) public health, (5) ecological environment, or (6) if loss or disruption impacts citizens or the government administration at a national scale.[31]

Critical infrastructure:

- Electrical power
- Electronic communication
- Water supply and sewage
- Transport
- Oil and gas
- Satellite Based infrastructure

Critical societal functions

- Banking and finance
- Food supply
- Health services, social services, and social security benefit
- The Police
- Emergency and rescue service
- Crisis management
- Parliament and government
- The Judiciary
- Defence
- Environmental surveillance
- Waste treatment[32]

New Zealand
Critical National Infrastructure (CNI) is defined as those systems and assets, whether physical or virtual, so vital to New Zealand that the incapacity or destruction of such systems and assets would have a debilitating impact on the security of the nation, the economy, public health and safety, or any combination of those matters.

• Emergency Services,
• Energy (including Electricity Generation and Distribution, and the Distribution of Oil and Gas),
• Finance and Banking,
• Governance (including Law and Order and National and Economic Security),
• Telecommunications and the Internet,
• Transport (including Air, Land, and Sea).[33]

[31] Norway. Protection of critical infrastructures and critical societal functions in Norway. , 1 Jul 2006.
[32] Ibid.

Poland
• Telecommunications,
• Energy,
• Banking and Finance,
• Transportation,
• Chemical Industry,
• Water and Sewage Systems,
• Private and governmental emergency services.[34]

Russia
• Economy,
• Domestic and Foreign Policy,
• Science and Technology,
• State Information and Communication Systems,
• Defense,
• Justice,
• Disaster Response.[35]

Singapore
• Banking and Finance,
• Information- and Telecommunications,
• Energy,
• Water,
• Transportation,
• Health.
• Aviation Security,
• Maritime Security.[36]

Spain
Those facilities, networks, services and hardware and information technology, the disruption or destruction would have a major impact on health, safety or the economic welfare of the citizens or the effective functioning of state institutions and Public Administration.[37]
• Chemical Industry,
• Nuclear Industry,
• Investigative installations,
• Centers of Power,
• Space,
• Energy sector,
• Telecommunications,

---

[33] "What is CNI?." Centre for Critical Infrastructure Protection. Government Communications Security Bureau, n.d. Web. 15 Apr 2011. <http://www.ccip.govt.nz/about-ccip/what-is-cni.html>.
[34] Brunner and Suter 321.
[35] Ibid 339.
[36] Ibid 359-360.
[37] Brunner and Suter.

• Transportation,
• Water supply,
• Alimentation,
• Financial Sector,
• Public Health.[38]

Sweden
• Air Control Systems,
• Supervisory Control And Data Acquisition (SCADA) systems in use within water, transport, and industry,
• Financial Systems,
• National Command Systems,
• Telecommunication Systems,
• The Internet.[39]

Switzerland
The collective term "infrastructures" covers people, organizations, processes, products, services, and information flows, as well as technical and structural installations and constructions that, individually or as part of a network, enable the society, the economy, and the state to function.
These infrastructures are grouped into three levels:
- Sectors: e.g., energy, financial services, public health
- Subsectors: e.g., power supply, oil supply, natural gas supply
- Individual objects/elements: e.g., control centre for grid management, control systems, high-voltage power lines, dams, pipelines
Critical infrastructures are infrastructures whose disruption, failure, or destruction would have a serious impact on public health, public and political affairs, the environment, security, and social and economic well-being.
The criticality of an infrastructure refers to its relative importance in terms of the consequences that a disruption, failure, or destruction would have on the population and its vital resources. [40]

United Kingdom
The national infrastructure comprises the facilities, systems, sites and networks necessary for the delivery of the essential services upon which daily life in the UK depends.
Critical national infrastructure
Not everything within a national infrastructure sector is 'critical'. In the sectors there are certain 'critical' elements of infrastructure, the loss or compromise of which would have a major, detrimental impact on the availability or integrity of essential services, leading to severe

[38] Ibid 372.
[39] Ibid 391.
[40] E-Government Unit, State Services Commission. "E-Government: Protecting New Zealand's Infrastructure from Cyber Threats", (December 2000). http://www.ccip.govt.nz/aboutccip/background/niip-report-final.pdf.

economic or social consequences or to loss of life. These 'critical' assets make up the nation's critical national infrastructure (CNI) and are referred to individually as 'infrastructure assets'. Infrastructure assets may be physical (e.g. sites, installations, pieces of equipment) or logical (e.g. information networks, systems).[41]

• Communications (Data Communications, Fixed Voice Communications, Mail, Public Information, Wireless Communications),
• Emergency Services (Ambulance, Fire and Rescue, Coastguard, Police),
• Energy (Electricity, Natural Gas, Petroleum),
• Finance (Asset Management, Financial Facilities, Investment Banking, Markets, Retail Banking),
• Food (Produce, Import, Process, Distribute, Retail),
• Government and Public Services (Central, Regional, and Local Government; Parliaments and Legislatures; Justice; National Security),
• Public Safety (Chemical, Biological, Radiological, and Nuclear (CBRN) Terrorism; Crowds and Mass Events),
• Health (Health Care, Public Health),
• Transport (Air, Marine, Rail, Road),
• Water (Mains Water, Sewerage).[42]

[41] United Kingdom. National Infrastructure. Centre for National Infrastructure Protection, Web. 5 Apr 2011. <http://www.cpni.gov.uk/about/cni/>.
[42] Ibid.

Methodology Questionnaire

Infrastructure sector examined: ____Emergency Response_____

Name of Interviewee: ____Tyler Eschbach_____

Title of interviewee: ____Communications Captain_____

Name of Interviewer: ____Andy Giblin_____

Date: ____4/20/2011_____

As outlined in the definitions, the infrastructure sector is integral in the missions of:

- ☐ National Security
- ☐ Economic Security
- ☐ X Public Safety

If National Security was checked:

What key missions of national security do the infrastructure sector affect/perform?

- ☐ Enables the conduct military operations
- ☐ Enables the conduct of foreign affairs
- ☐ Enables intelligence cycle
- ☐ Enables the conduct of judiciary bodies
- ☐ Enables effective governance

For those checked:

Which of these components of ***the conduct of military affairs*** does the infrastructure sector perform?

- ☐ Transportation of military personnel to and within operational areas abroad
- ☐ Communication between operational elements and command

- ☐ Procurement of needed weapons and resources
- ☐ Military response to national states of emergency
- ☐ Coordination and communication between military and allies

Which of these components of ***the conduct of foreign affairs*** does the infrastructure sector perform?

- ☐ Communication of diplomatic instructions to tasked government personnel abroad
- ☐ Communication with foreign government representatives on international policy
- ☐ Deployment of diplomatic personnel to other areas
- ☐ Security of diplomatic personnel abroad
- ☐ Secure transportation of the President or high-level government officialsoverseas

Which of these components of the ***intelligence cycle*** does the infrastructure sector perform?

- ☐ Tasking of needed intelligence
- ☐ Intelligence collection (HUMINT, SIGNIT, IMINT, etc)
- ☐ Intelligence processing (decoding, translation, etc)
- ☐ Intelligence analysis
- ☐ Intelligence dissemination to appropriate parties

Which of the components of **the conduct of judicial bodies** does the infrastructure sector perform?

- ☐ Maintaining the integrity of evidence for civil cases
- ☐ Maintaining integrity of evidence for criminal cases
- ☐ Enabling the trying of cases within courtroom
- ☐ Maintaining integrity of legal documentation
- ☐ Communication between trial, appellate, state supreme, and supreme courts

Which of the components of ***effective governance*** does the infrastructure sector perform?

- ☐ General populace giving feedback to government
- ☐ Holding of elections
- ☐ Tallying and computing results of elections
- ☐ Communication of policy, laws, or intentions to wider populace
- ☐ Communication between local, federal, state, and national levels of government

---

If Economic Security was checked:

What key missions of economic security do the infrastructure sector affect/perform?

- ☐ Enabling the security of monetary and financial data
- ☐ Enabling the flow of monetary and financial data
- ☐ Enabling the integrity of monetary and financial data
- ☐ Enabling the security, flow, and integrity of goods and services through international trade
- ☐ Enabling the security, flow, and integrity of goods and services through inter-state trade

For those checked:

Which of these components of the ***security of monetary and financial data*** does the infrastructure sector perform?

- ☐ Preventing removal of funds from companies by non-authorized individuals
- ☐ Preventing access to personal data by non-authorized individuals
- ☐ Preventing access to address/phone numbers/SSNs/insurance numbers by non-authorized individuals.
- ☐ Preventing access to financial statements and/or company data by unauthorized users
- ☐ Preventing access to data relating to exchanges and stock markets by unauthorized users.

Which of these components of the ***flow of monetary and financial data*** does the infrastructure sector perform?

- ☐ Maintaining functionality of credit card and electronic systems

- ☐ Enabling customers to deposit and/or withdraw funds
- ☐ Enabling banks to transfer funds between each other
- ☐ Preventing runs on banks
- ☐ Preventing the value of the dollar from being artificially impacted compared to other currencies

Which of these components of the ***integrity of monetary and financial data*** does the infrastructure sector perform?

- ☐ Preventing monetary and financial data from being destroyed
- ☐ Ensuring the accuracy of banks' records of holdings
- ☐ Ensuring individuals' personal information is not maliciously altered
- ☐ Ensuring banks' customer data is not altered
- ☐ Maintaining accuracy of data relating to exchanges and stock markets

Which of these components of the ***security, flow, and integrity of goods and services through international trade*** does the infrastructure sector perform?

- ☐ Functionality of oil and gas pipelines
- ☐ Preventing the malicious disruption of supply chain management systems
- ☐ Preventing the disruption of sea transportation
- ☐ Preventing the disruption of land transportation
- ☐ Preventing the disruption of air transportation

Which of these components of the ***security, flow, and integrity of goods and services through inter-state trade*** does the infrastructure sector perform?

- ☐ Functionality of oil and gas pipelines
- ☐ Preventing the malicious disruption of supply chain management systems
- ☐ Preventing the disruption of sea transportation
- ☐ Preventing the disruption of land transportation

☐ Preventing the disruption of air transportation

If Public Safety was checked:

What key missions of public safety do the infrastructure sector affect/perform?

☐ X Disease outbreak prevention and mitigation

☐ X Timely emergency services

☐ State and local law enforcement presence/response

☐ Access to basic needs

For those checked:

Which of these components of ***disease outbreak prevention and mitigation*** does the infrastructure sector perform?

☐ Dissemination of necessary medicinal supplies cannot be disseminated among the population.

☐ Identifying and, if needed, quarantining infected individuals

☐ Communication of necessary preventative measures to general public

☐ Communication of general population with public health authorities

☐ X Ensuring access to patient records

Which of these components of ***timely emergency services*** does the infrastructure sector perform?

☐ *X Notification of an incident to* emergency responders

☐ X Access of emergency responders to affected area

☐ X Access adequate supplies and equipment for emergency responders

☐ X Transportation by emergency responders cannot of victims

☐ X Communication between emergency responder elements

Which of these components of ***state/local law enforcement presence and response*** does the infrastructure sector perform?

- ☐ Communication and assessment of alerts from general population of criminal activity
- ☐ Communication between law enforcement elements
- ☐ Access to affected area
- ☐ Physically apprehension of perpetrators
- ☐ Incarceration of perpetrators

Which of these components of ***access to basic needs*** does the infrastructure sector perform?

- ☐ General population access to clean water.
- ☐ General population having shelter against adverse weather.
- ☐ General population access to a safe air supply.
- ☐ General population protection from adverse radiological or chemical elements.
- ☐ General population protection from unsafe structures or environments that threaten physical harm

---

Complete the following for each component checked underneath the red headings.

Key mission: ___Public Safety_____

Component: ___All Checked_____

Does the component currently depend on cyber assets?	Y	N
If YES:		
Is there a human or mechanical backup to adequately and quickly replace the functions of the cyber assets?	Y	N

If NO:

Should the component be lost due to destruction or manipulation of cyber assets, how many people would experience **loss of life**?

>10,000	1,000 - 10,000	100-1,000	50-100	<50	None

Should the component be lost due to destruction or manipulation of cyber assets, how many people would experience **severe injuries/illness**?

>10,000	1,000 - 10,000	100-1,000	50-100	<50	None

Should the component be lost due to destruction or manipulation of cyber assets, how many people would experience **minor injuries/illness**?

>10,000	1,000 - 10,000	100-1,000	50-100	<50	None

Should the component be lost due to destruction or manipulation of cyber assets, how many people would experience **inconvenience**?

>10,000	1,000 - 10,000	100-1,000	50-100	<50	None

What is the estimated recovery time of the cyber assets?

Years	Months	Days	Hours	Minutes	Seconds

What is the estimated time length of the immediate, primary effects upon [national security,

economic security, or public safety]?

Years Months Days Hours Minutes Seconds

There is a backup to the cyber assets relied upon by emergency responders, which is radio dispatch, but as this could take a couple of hours to fully and effectively implement, we put that there is no backup and that it would take hours to restore functionality.

Our source selected all responses checked.

Methodology Questionnaire

Infrastructure sector examined: ___IT_____

Name of Interviewee: ___Willis Marti_____

Title of interviewee: Director, Networking and Chief Information Security Officer

Name of Interviewer: ___George Stasny_____

Date: ___4/13/2011_____

As outlined in the definitions, the infrastructure sector is integral in the missions of:

- ☐ National Security
- ☐ X Economic Security
- ☐ Public Safety

If National Security was checked:

What key missions of national security do the infrastructure sector affect/perform?

- ☐ Enables the conduct military operations
- ☐ Enables the conduct of foreign affairs
- ☐ Enables intelligence cycle
- ☐ Enables the conduct of judiciary bodies
- ☐ Enables effective governance

For those checked:

Which of these components of ***the conduct of military affairs*** does the infrastructure sector perform?

- ☐ Transportation of military personnel to and within operational areas abroad
- ☐ Communication between operational elements and command

- ☐ Procurement of needed weapons and resources
- ☐ Military response to national states of emergency
- ☐ Coordination and communication between military and allies

Which of these components of ***the conduct of foreign affairs*** does the infrastructure sector perform?

- ☐ Communication of diplomatic instructions to tasked government personnel abroad
- ☐ Communication with foreign government representatives on international policy
- ☐ Deployment of diplomatic personnel to other areas
- ☐ Security of diplomatic personnel abroad
- ☐ Secure transportation of the President or high-level government officialsoverseas

Which of these components of the ***intelligence cycle*** does the infrastructure sector perform?

- ☐ Tasking of needed intelligence
- ☐ Intelligence collection (HUMINT, SIGNIT, IMINT, etc)
- ☐ Intelligence processing (decoding, translation, etc)
- ☐ Intelligence analysis
- ☐ Intelligence dissemination to appropriate parties

Which of the functions of **the conduct of judicial bodies** does the infrastructure sector perform?

- ☐ Maintaining the integrity of evidence for civil cases
- ☐ Maintaining integrity of evidence for criminal cases
- ☐ Enabling the trying of cases within courtroom
- ☐ Maintaining integrity of legal documentation
- ☐ Communication between trial, appellate, state supreme, and supreme courts

Which of the functions of ***effective governance*** does the infrastructure sector perform?

- ☐ General populace giving feedback to government

- ☐ Holding of elections
- ☐ Tallying and computing results of elections
- ☐ Communication of policy, laws, or intentions to wider populace
- ☐ Communication between local, federal, state, and national levels of government

---

If Economic Security was checked:

What key missions of economic security do the infrastructure sector affect/perform?

- ☐ X Enabling the security of monetary and financial data
- ☐ X Enabling the flow of monetary and financial data
- ☐ X Enabling the integrity of monetary and financial data
- ☐ Enabling the security, flow, and integrity of goods and services through international trade
- ☐ Enabling the security, flow, and integrity of goods and services through inter-state trade

For those checked:

Which of these components of the ***security of monetary and financial data*** does the infrastructure sector perform?

- ☐ X Preventing removal of funds from companies by non-authorized individuals
- ☐ X Preventing access to personal data by non-authorized individuals
- ☐ X Preventing access to address/phone numbers/SSNs/insurance numbers by non-authorized individuals.
- ☐ Preventing access to financial statements and/or company data by unauthorized users
- ☐ Preventing access to data relating to exchanges and stock markets by unauthorized users.

Which of these components of the ***flow of monetary and financial data*** does the infrastructure sector perform?

- ☐ X Maintaining functionality of credit card and electronic systems

- ☐ Enabling customers to deposit and/or withdraw funds
- ☐ Enabling banks to transfer funds between each other
- ☐ Preventing runs on banks
- ☐ Preventing the value of the dollar from being artificially impacted compared to other currencies

Which of these components of the ***integrity of monetary and financial data*** does the infrastructure sector perform?

- ☐ X Preventing monetary and financial data from being destroyed
- ☐ X Ensuring the accuracy of banks' records of holdings
- ☐ X Ensuring individuals' personal information is not maliciously altered
- ☐ Ensuring banks' customer data is not altered
- ☐ Maintaining accuracy of data relating to exchanges and stock markets

Which of these components of the ***security, flow, and integrity of goods and services through international trade*** does the infrastructure sector perform?

- ☐ Functionality of oil and gas pipelines
- ☐ Preventing the malicious disruption of supply chain management systems
- ☐ Preventing the disruption of sea transportation
- ☐ Preventing the disruption of land transportation
- ☐ Preventing the disruption of air transportation

If Public Safety was checked:

What key missions of public safety do the infrastructure sector affect/perform?

- ☐ Disease outbreak prevention and mitigation
- ☐ Timely emergency services
- ☐ State and local law enforcement presence/response

☐ Access to basic needs

For those checked:

Which of these components of ***disease outbreak prevention and mitigation*** does the infrastructure sector perform?

☐ Dissemination of necessary medicinal supplies cannot be disseminated among the population.

☐ Identifying and, if needed, quarantining infected individuals

☐ Communication of necessary preventative measures to general public

☐ Communication of general population with public health authorities

☐ Ensuring access to patient records

Which of these components of ***timely emergency services*** does the infrastructure sector perform?

☐ *Notification of an incident to* emergency responders

☐ Access of emergency responders to affected area

☐ Access adequate supplies and equipment for emergency responders

☐ Transportation by emergency responders cannot of victims

☐ Communication between emergency responder elements

☐ Communication and assessment of alerts from general population of criminal activity

☐ Communication between law enforcement elements

☐ Access to affected area

☐ Physically apprehension of perpetrators

☐ Incarceration of perpetrators

Which of these components of ***access to basic needs*** does the infrastructure sector perform?

☐ General population access to clean water.

☐ General population having shelter against adverse weather.

☐ General population access to a safe air supply.

☐ General population protection from adverse radiological or chemical elements.

☐ General population protection from unsafe structures or environments that threaten physical harm

---

Complete the following for each component checked underneath the red headings.

Key mission: ___All Economic Security_____

Component: _____

Does the component currently depend on cyber assets? Y N

If YES:

Is there a human or mechanical backup to adequately and quickly replace the functions of the cyber assets? Y N

If NO:

Should the component be lost due to destruction or manipulation of cyber assets, how many people would experience **loss of life**?

>10,000 1,000 - 10,000 100-1,000 50-100 <50 None

Should the component be lost due to destruction or manipulation of cyber assets, how many people would experience **severe injuries/illness**?

>10,000 1,000 - 10,000 100-1,000 50-100 <50 None

Should the component be lost due to destruction or manipulation of cyber assets, how many people would experience **minor injuries/illness**?

>10,000 1,000 - 10,000 100-1,000 50-100 <50 None

Should the component be lost due to destruction or manipulation of cyber assets, how many people would experience **inconvenience**?

>10,000 1,000 - 10,000 100-1,000 50-100 <50 None

What is the estimated recovery time of the cyber assets?

Years Months Days Hours Minutes Seconds

What is the estimated time length of the immediate, primary effects upon [national security,

economic security, or public safety]?

Years Months Days Hours Minutes Seconds

Notes on interview:

The IT department at Texas A&M uses two server rooms, one located in the Teague building on Main Campus (east of Wellborn Rd.) with the other in the Wehner building on West Campus. There is hosting redundancy between these two server rooms, though off-campus connectivity is routed entirely through the Wehner facility. From there, fiber optic cables run west toward Easterwood airport until they hit a data trunk that runs north the Dallas/Fort Worth as well as south to Houston. Severing this line before it gets to Wehner would eliminate any connection between campus and the wider internet, though the estimate for repair time given a simple cut is measured in hours.

Should critical damage occur on the server rooms themselves, there is secure offsite backup hosted in Dallas, and full contingency plans are in place to restore all missing or corrupted data within 72 hours. Should an outage occur during paycheck disbursal, the plan is to pay employees based on the previous month's earnings, for which there are paper records, and reconcile any differences once the system is back on line. The greatest damage would arise if there is a severe outage in the time immediately preceding graduation. This could result in a delay in degrees being awarded, as grade information would be temporarily unavailable.

For Texas A&M, given the contingency plans in place, the maximum level of damage would be inconvenience, and any problem would likely be remedied with a few days.

Willis Marti bio:

Willis Marti is the Director, Networking and Chief Information Security Officer at Texas A&M University. He is also the Associate Director of the Academy for Advanced Telecommunications and Learning Technologies, and a Senior Lecturer in the Computer Science Department.

Mr. Marti has been instrumental in Campus Network improvements, the creation of the Lone Star Education and Research Network (LEARN), and the development of a partnership with the University of Texas to create resilient networking for both schools. In addition, he assisted in the founding of the IT Forum and the IT Advisory Committee.

Mr. Marti also initiated the Virtual Network Engineering Laboratory and serves as Co-Principle Investigator for the related NSF grant. He assisted in the development of a successful proposal naming Texas A&M University as a Center of Academic Excellence by the National Security Agency. He also sponsors Texas A&M's nationally recognized Collegiate Cyber Defense Competition (CCDC) Team.

Mr. Marti holds a Bachelor of Science from the United States Military Academy, and a Master of Science in Computer Science from Stanford University.

Methodology Questionnaire

Infrastructure sector examined: _____Nuclear Facility_____

Name of Interviewee: _____Dr. William Charlton_____

Title of interviewee: __Director of NSSPI & Professor of nuclear engineering

Name of Interviewer: _____Aimee Anderson & Matt Jennings_____

Date: _____4/21/2011_____

As outlined in the definitions, the infrastructure sector is integral in the missions of:

- ☐ National Security
- ☐ Economic Security
- ☐ X Public Safety

If National Security was checked:

What key missions of national security do the infrastructure sector affect/perform?

- ☐ Enables the conduct military operations
- ☐ Enables the conduct of foreign affairs
- ☐ Enables intelligence cycle
- ☐ Enables the conduct of judiciary bodies
- ☐ Enables effective governance

For those checked:

Which of these components of ***the conduct of military affairs*** does the infrastructure sector perform?

- ☐ Transportation of military personnel to and within operational areas abroad
- ☐ Communication between operational elements and command

- ☐ Procurement of needed weapons and resources
- ☐ Military response to national states of emergency
- ☐ Coordination and communication between military and allies

Which of these components of ***the conduct of foreign affairs*** does the infrastructure sector perform?

- ☐ Communication of diplomatic instructions to tasked government personnel abroad
- ☐ Communication with foreign government representatives on international policy
- ☐ Deployment of diplomatic personnel to other areas
- ☐ Security of diplomatic personnel abroad
- ☐ Secure transportation of the President or high-level government officialsoverseas

Which of these components of the ***intelligence cycle*** does the infrastructure sector perform?

- ☐ Tasking of needed intelligence
- ☐ Intelligence collection (HUMINT, SIGNIT, IMINT, etc)
- ☐ Intelligence processing (decoding, translation, etc)
- ☐ Intelligence analysis
- ☐ Intelligence dissemination to appropriate parties

Which of the components of **the conduct of judicial bodies** does the infrastructure sector perform?

- ☐ Maintaining the integrity of evidence for civil cases
- ☐ Maintaining integrity of evidence for criminal cases
- ☐ Enabling the trying of cases within courtroom
- ☐ Maintaining integrity of legal documentation
- ☐ Communication between trial, appellate, state supreme, and supreme courts

Which of the components of ***effective governance*** does the infrastructure sector perform?

- ☐ General populace giving feedback to government
- ☐ Holding of elections
- ☐ Tallying and computing results of elections
- ☐ Communication of policy, laws, or intentions to wider populace
- ☐ Communication between local, federal, state, and national levels of government

---

If Economic Security was checked:

What key missions of economic security do the infrastructure sector affect/perform?

- ☐ Enabling the security of monetary and financial data
- ☐ Enabling the flow of monetary and financial data
- ☐ Enabling the integrity of monetary and financial data
- ☐ Enabling the security, flow, and integrity of goods and services through international trade
- ☐ Enabling the security, flow, and integrity of goods and services through inter-state trade

For those checked:

Which of these components of the ***security of monetary and financial data*** does the infrastructure sector perform?

- ☐ Preventing removal of funds from companies by non-authorized individuals
- ☐ Preventing access to personal data by non-authorized individuals
- ☐ Preventing access to address/phone numbers/SSNs/insurance numbers by non-authorized individuals.
- ☐ Preventing access to financial statements and/or company data by unauthorized users
- ☐ Preventing access to data relating to exchanges and stock markets by unauthorized users.

Which of these components of the ***flow of monetary and financial data*** does the infrastructure sector perform?

- ☐ Maintaining functionality of credit card and electronic systems

- ☐ Enabling customers to deposit and/or withdraw funds
- ☐ Enabling banks to transfer funds between each other
- ☐ Preventing runs on banks
- ☐ Preventing the value of the dollar from being artificially impacted compared to other currencies

Which of these components of the ***integrity of monetary and financial data*** does the infrastructure sector perform?

- ☐ Preventing monetary and financial data from being destroyed
- ☐ Ensuring the accuracy of banks' records of holdings
- ☐ Ensuring individuals' personal information is not maliciously altered
- ☐ Ensuring banks' customer data is not altered
- ☐ Maintaining accuracy of data relating to exchanges and stock markets

Which of these components of the ***security, flow, and integrity of goods and services through international trade*** does the infrastructure sector perform?

- ☐ Functionality of oil and gas pipelines
- ☐ Preventing the malicious disruption of supply chain management systems
- ☐ Preventing the disruption of sea transportation
- ☐ Preventing the disruption of land transportation
- ☐ Preventing the disruption of air transportation

Which of these components of the ***security, flow, and integrity of goods and services through inter-state trade*** does the infrastructure sector perform?

- ☐ Functionality of oil and gas pipelines
- ☐ Preventing the malicious disruption of supply chain management systems
- ☐ Preventing the disruption of sea transportation
- ☐ Preventing the disruption of land transportation

☐ Preventing the disruption of air transportation

If Public Safety was checked:

What key missions of public safety do the infrastructure sector affect/perform?

☐ X Disease outbreak prevention and mitigation

☐ X Timely emergency services

☐ State and local law enforcement presence/response

☐ Access to basic needs

For those checked:

Which of these components of ***disease outbreak prevention and mitigation*** does the infrastructure sector perform?

☐ X Dissemination of necessary medicinal supplies cannot be disseminated among the population.

☐ Identifying and, if needed, quarantining infected individuals

☐ Communication of necessary preventative measures to general public

☐ Communication of general population with public health authorities

☐ Ensuring access to patient records

Which of these components of ***timely emergency services*** does the infrastructure sector perform?

☐ *Notification of an incident to* emergency responders

☐ Access of emergency responders to affected area

☐ Access adequate supplies and equipment for emergency responders

☐ Transportation by emergency responders cannot of victims

☐ Communication between emergency responder elements

Which of these components of ***state/local law enforcement presence and response*** does the infrastructure sector perform?

- ☐ Communication and assessment of alerts from general population of criminal activity
- ☐ Communication between law enforcement elements
- ☐ Access to affected area
- ☐ Physically apprehension of perpetrators
- ☐ Incarceration of perpetrators

Which of these components of ***access to basic needs*** does the infrastructure sector perform?

- ☐ General population access to clean water.
- ☐ General population having shelter against adverse weather.
- ☐ General population access to a safe air supply.
- ☐ General population protection from adverse radiological or chemical elements.
- ☐ General population protection from unsafe structures or environments that threaten physical harm

---

Complete the following for each component checked underneath the red headings.

Key mission: ____Public Safety_____

Component: ____All checked_____

Does the component currently depend on cyber assets? Y N

If YES:

Is there a human or mechanical backup to adequately and quickly replace the functions of the cyber assets? Y N

If NO:

Should the component be lost due to destruction or manipulation of cyber assets, how many people would experience **loss of life**?

>10,000 1,000 - 10,000 100-1,000 50-100 <50 None

Should the component be lost due to destruction or manipulation of cyber assets, how many people would experience **severe injuries/illness**?

>10,000 1,000 - 10,000 100-1,000 50-100 <50 None

Should the component be lost due to destruction or manipulation of cyber assets, how many people would experience **minor injuries/illness**?

>10,000 1,000 - 10,000 100-1,000 50-100 <50 None

Should the component be lost due to destruction or manipulation of cyber assets, how many people would experience **inconvenience**?

>10,000 1,000 - 10,000 100-1,000 50-100 <50 None

What is the estimated recovery time of the cyber assets?

Years Months Days Hours Minutes Seconds

(Time estimated to implement backup)

What is the estimated time length of the immediate, primary effects upon [national security, economic security, or public safety]?

Years	Months	Days	Hours	Minutes	Seconds

Quick bio of Charlton (from http://nsspi.tamu.edu/people/professional-staff)

Dr. Charlton serves as the Director of NSSPI and as such directs the overall NSSPI activities. Dr. Charlton is an expert in the area of nuclear nonproliferation research and education. Prior to his appointment at TAMU, he was an Assistant Professor in the Nuclear and Radiation Engineering Program at the University of Texas at Austin from 2000-2003. From 1998-2000, Dr. Charlton was a Technical Staff Member in the Nonproliferation and International Security Division at Los Alamos National Laboratory (LANL). He remains heavily involved with many of the National Laboratories including: consultation on nuclear material safeguards and national security projects, providing graduate and undergraduate students for summer programs and new hires, collaborating with laboratory staff on various funded research projects, and helping to provide continuing education opportunities for laboratory employees. He teaches courses which study the technical aspects of nuclear nonproliferation, safeguards, and nuclear security as well as fundamentals of nuclear engineering. Dr. Charlton earned a Ph.D. in Nuclear Engineering from Texas A&M University. Among his many awards, Dr. Charlton was named the George Armistead Jr. '23 Faculty Fellow at TAMU in 2005, was awarded the Dwight Look College of Engineering Faculty Fellow in 2007, was recognized as the Advisor of the Year by the TAMU Division of Student Affairs in 2009, and earned the Special Service Award from the Institute of Nuclear Materials Management in 2010. Dr. Charlton is recognized as one of the leaders in the technical area of nuclear nonproliferation education and research. He has over 150 technical publications in refereed journals and conference proceedings.

Notes on his survey answers

Dr. Charlton's answers on our survey relate to the nuclear research reactor on the Texas A&M campus and not to nuclear facilities in general. He noted that different kinds of nuclear reactors will have different types of consequences if their cyber assets were to be disabled. The primary function of Texas A&M's research reactor is to produce medical isotopes for cancer treatments at hospitals in Houston, TX. For this reason, the consequences, according to Dr. Charlton's answers, relate only to public safety and, more specifically disease outbreak mitigation (check the survey – I'm not sure if he checked another box here). In contrast, Dr. Charlton mentioned that larger nuclear weapons facilities will have a much greater impact on national security than public safety if it were to lose its cyber assets.

Methodology Questionnaire

Infrastructure sector examined: ____Utilities and Energy Management_____

Name of Interviewee: ____David Brown_____

Title of interviewee: ____Senior Lead Systems Engineer_____

Name of Interviewer: ____Steph Shaffer_____

Date: ____4/20/2011_____

As outlined in the definitions, the infrastructure sector is integral in the missions of:

- ☐ National Security
- ☐ X Economic Security
- ☐ X Public Safety

If National Security was checked:

What key missions of national security do the infrastructure sector affect/perform?

- ☐ Enables the conduct military operations
- ☐ Enables the conduct of foreign affairs
- ☐ Enables intelligence cycle
- ☐ Enables the conduct of judiciary bodies
- ☐ Enables effective governance

For those checked:

Which of these components of ***the conduct of military affairs*** does the infrastructure sector perform?

- ☐ Transportation of military personnel to and within operational areas abroad
- ☐ Communication between operational elements and command

- ☐ Procurement of needed weapons and resources
- ☐ Military response to national states of emergency
- ☐ Coordination and communication between military and allies

Which of these components of ***the conduct of foreign affairs*** does the infrastructure sector perform?

- ☐ Communication of diplomatic instructions to tasked government personnel abroad
- ☐ Communication with foreign government representatives on international policy
- ☐ Deployment of diplomatic personnel to other areas
- ☐ Security of diplomatic personnel abroad
- ☐ Secure transportation of the President or high-level government officialsoverseas

Which of these components of the ***intelligence cycle*** does the infrastructure sector perform?

- ☐ Tasking of needed intelligence
- ☐ Intelligence collection (HUMINT, SIGNIT, IMINT, etc)
- ☐ Intelligence processing (decoding, translation, etc)
- ☐ Intelligence analysis
- ☐ Intelligence dissemination to appropriate parties

Which of the components of **the conduct of judicial bodies** does the infrastructure sector perform?

- ☐ Maintaining the integrity of evidence for civil cases
- ☐ Maintaining integrity of evidence for criminal cases
- ☐ Enabling the trying of cases within courtroom
- ☐ Maintaining integrity of legal documentation
- ☐ Communication between trial, appellate, state supreme, and supreme courts

Which of the components of ***effective governance*** does the infrastructure sector perform?

- ☐ General populace giving feedback to government
- ☐ Holding of elections
- ☐ Tallying and computing results of elections
- ☐ Communication of policy, laws, or intentions to wider populace
- ☐ Communication between local, federal, state, and national levels of government

---

If Economic Security was checked:

What key missions of economic security do the infrastructure sector affect/perform?

- ☐ X Enabling the security of monetary and financial data
- ☐ X Enabling the flow of monetary and financial data
- ☐ X Enabling the integrity of monetary and financial data
- ☐ Enabling the security, flow, and integrity of goods and services through international trade
- ☐ Enabling the security, flow, and integrity of goods and services through inter-state trade

For those checked:

Which of these components of the ***security of monetary and financial data*** does the infrastructure sector perform?

- ☐ Preventing removal of funds from companies by non-authorized individuals
- ☐ X Preventing access to personal data by non-authorized individuals
- ☐ X Preventing access to address/phone numbers/SSNs/insurance numbers by non-authorized individuals.
- ☐ X Preventing access to financial statements and/or company data by unauthorized users
- ☐ Preventing access to data relating to exchanges and stock markets by unauthorized users.

Which of these components of the ***flow of monetary and financial data*** does the infrastructure sector perform?

- ☐ Maintaining functionality of credit card and electronic systems

- ☐ Enabling customers to deposit and/or withdraw funds
- ☐ Enabling banks to transfer funds between each other
- ☐ Preventing runs on banks
- ☐ Preventing the value of the dollar from being artificially impacted compared to other currencies

Which of these components of the ***integrity of monetary and financial data*** does the infrastructure sector perform?

- ☐ X Preventing monetary and financial data from being destroyed
- ☐ Ensuring the accuracy of banks' records of holdings
- ☐ X Ensuring individuals' personal information is not maliciously altered
- ☐ Ensuring banks' customer data is not altered
- ☐ Maintaining accuracy of data relating to exchanges and stock markets

Which of these components of the ***security, flow, and integrity of goods and services through international trade*** does the infrastructure sector perform?

- ☐ X Functionality of oil and gas pipelines
- ☐ X Preventing the malicious disruption of supply chain management systems
- ☐ Preventing the disruption of sea transportation
- ☐ Preventing the disruption of land transportation
- ☐ Preventing the disruption of air transportation

Which of these components of the ***security, flow, and integrity of goods and services through inter-state trade*** does the infrastructure sector perform?

- ☐ Functionality of oil and gas pipelines
- ☐ Preventing the malicious disruption of supply chain management systems
- ☐ Preventing the disruption of sea transportation
- ☐ Preventing the disruption of land transportation

☐ Preventing the disruption of air transportation

If Public Safety was checked:

What key missions of public safety do the infrastructure sector affect/perform?

☐ X Disease outbreak prevention and mitigation

☐ Timely emergency services

☐ X State and local law enforcement presence/response

☐ X Access to basic needs

For those checked:

Which of these components of ***disease outbreak prevention and mitigation*** does the infrastructure sector perform?

☐ Dissemination of necessary medicinal supplies cannot be disseminated among the population.

☐ Identifying and, if needed, quarantining infected individuals

☐ X Communication of necessary preventative measures to general public

☐ X Communication of general population with public health authorities

☐ Ensuring access to patient records

Which of these components of ***timely emergency services*** does the infrastructure sector perform?

☐ *X Notification of an incident to* emergency responders

☐ X Access of emergency responders to affected area

☐ Access adequate supplies and equipment for emergency responders

☐ Transportation by emergency responders cannot of victims

☐ X Communication between emergency responder elements

Which of these components of ***state/local law enforcement presence and response*** does the infrastructure sector perform?

- ☐ X Communication and assessment of alerts from general population of criminal activity
- ☐ Communication between law enforcement elements
- ☐ X Access to affected area
- ☐ Physically apprehension of perpetrators
- ☐ Incarceration of perpetrators

Which of these components of ***access to basic needs*** does the infrastructure sector perform?

- ☐ X General population access to clean water.
- ☐ General population having shelter against adverse weather.
- ☐ X General population access to a safe air supply.
- ☐ General population protection from adverse radiological or chemical elements.
- ☐ X General population protection from unsafe structures or environments that threaten physical harm

---

Complete the following for each component checked underneath the red headings.

Key mission: __Econ Security_____

Component: ____All checked_____

Does the component currently depend on cyber assets?	Y	N
If YES:		
Is there a human or mechanical backup to adequately and quickly replace the functions of the cyber assets?	Y	N

If NO:

Should the component be lost due to destruction or manipulation of cyber assets, how many people would experience **loss of life**?

>10,000	1,000 - 10,000	100-1,000	50-100	<50	None

Should the component be lost due to destruction or manipulation of cyber assets, how many people would experience **severe injuries/illness**?

>10,000	1,000 - 10,000	100-1,000	50-100	<50	None

Should the component be lost due to destruction or manipulation of cyber assets, how many people would experience **minor injuries/illness**?

>10,000	1,000 - 10,000	100-1,000	50-100	<50	None

Should the component be lost due to destruction or manipulation of cyber assets, how many people would experience **inconvenience**?

>10,000	1,000 - 10,000	100-1,000	50-100	<50	None

What is the estimated recovery time of the cyber assets?

Years	Months	Days	Hours	Minutes	Seconds

What is the estimated time length of the immediate, primary effects upon [national security,

economic security, or public safety]?

Years	Months	Days	Hours	Minutes	Seconds

Complete the following for each component checked underneath the red headings.

Key mission: __Public Safety_____

Component: ____All checked_____

Does the component currently depend on cyber assets?	Y	N

If YES:

Is there a human or mechanical backup to adequately and quickly replace the functions of the cyber assets?	Y	N

If NO:

Should the component be lost due to destruction or manipulation of cyber assets, how many people would experience **loss of life**?

>10,000	1,000 - 10,000	100-1,000	50-100	<50	None

Should the component be lost due to destruction or manipulation of cyber assets, how many people would experience **severe injuries/illness**?

>10,000	1,000 - 10,000	100-1,000	50-100	<50	None

Should the component be lost due to destruction or manipulation of cyber assets, how many people would experience **minor injuries/illness**?

>10,000	1,000 - 10,000	100-1,000	50-100	<50	None

Should the component be lost due to destruction or manipulation of cyber assets, how many people would experience **inconvenience**?

>10,000	1,000 - 10,000	100-1,000	50-100	<50	None

What is the estimated recovery time of the cyber assets?

Years Months Days Hours Minutes Seconds

What is the estimated time length of the immediate, primary effects upon [national security, economic security, or public safety]?

Years Months Days Hours Minutes Seconds

Notes on Interview

For the majority of functions performed by the Utilities and Energy Management Department at Texas A&M, it was determined that reliable backups to cyber assets exist; for example, the largest and most significant buildings on campus all have backup generators. For those functions which are not adequately backed-up, estimates of effect varied based on the type of cyber-attack. For an attack which merely disrupts functionality, the resetting of firmware and rebooting process should have functions restored within minutes. Recovery time is less well-known for cyber-attacks that cause damage to physical components, such as stuxnet-type viruses, as this type of attack has never occurred to the knowledge of our subject-matter expert. These types of concerns raise the criticality estimate for this particular sector.

Methodology Questionnaire

Infrastructure sector examined: __Transportation_____

Name of Interviewee: __John Happ_____

Title of interviewee: __Director of Aviation, Easterwood Airport_____

Name of Interviewer: __Shelley Nauss_____

Date: __April 11, 2011_____

As outlined in the definitions, the infrastructure sector is integral in the missions of:

- ☐ National Security
- ■ ☐ Economic Security
- ☐ Public Safety

If National Security was checked:

What key missions of national security do the infrastructure sector affect/perform?

- ☐ Enables the conduct military operations
- ☐ Enables the conduct of foreign affairs
- ☐ Enables intelligence cycle
- ☐ Enables the conduct of judiciary bodies
- ☐ Enables effective governance

For those checked:

Which of these components of ***the conduct of military affairs*** does the infrastructure sector perform?

- ☐ Transportation of military personnel to and within operational areas abroad
- ☐ Communication between operational elements and command
- ☐ Procurement of needed weapons and resources

☐ Military response to national states of emergency

☐ Coordination and communication between military and allies

Which of these components of ***the conduct of foreign affairs*** does the infrastructure sector perform?

☐ Communication of diplomatic instructions to tasked government personnel abroad

☐ Communication with foreign government representatives on international policy

☐ Deployment of diplomatic personnel to other areas

☐ Security of diplomatic personnel abroad

☐ Secure transportation of the President or high-level government officialsoverseas

Which of these components of the ***intelligence cycle*** does the infrastructure sector perform?

☐ Tasking of needed intelligence

☐ Intelligence collection (HUMINT, SIGNIT, IMINT, etc)

☐ Intelligence processing (decoding, translation, etc)

☐ Intelligence analysis

☐ Intelligence dissemination to appropriate parties

Which of the components of **the conduct of judicial bodies** does the infrastructure sector perform?

☐ Maintaining the integrity of evidence for civil cases

☐ Maintaining integrity of evidence for criminal cases

☐ Enabling the trying of cases within courtroom

☐ Maintaining integrity of legal documentation

☐ Communication between trial, appellate, state supreme, and supreme courts

Which of the components of ***effective governance*** does the infrastructure sector perform?

☐ General populace giving feedback to government

☐ Holding of elections

☐ Tallying and computing results of elections

☐ Communication of policy, laws, or intentions to wider populace

☐ Communication between local, federal, state, and national levels of government

---

If Economic Security was checked:

What key missions of economic security do the infrastructure sector affect/perform?

☐ Enabling the security of monetary and financial data

☐ Enabling the flow of monetary and financial data

☐ Enabling the integrity of monetary and financial data

■ ☐ Enabling the security, flow, and integrity of goods and services through international trade

■ ☐ Enabling the security, flow, and integrity of goods and services through inter-state trade

For those checked:

Which of these components of the ***security of monetary and financial data*** does the infrastructure sector perform?

☐ Preventing removal of funds from companies by non-authorized individuals

☐ Preventing access to personal data by non-authorized individuals

☐ Preventing access to address/phone numbers/SSNs/insurance numbers by non-authorized individuals.

☐ Preventing access to financial statements and/or company data by unauthorized users

☐ Preventing access to data relating to exchanges and stock markets by unauthorized users.

Which of these components of the ***flow of monetary and financial data*** does the infrastructure sector perform?

☐ Maintaining functionality of credit card and electronic systems

☐ Enabling customers to deposit and/or withdraw funds

☐ Enabling banks to transfer funds between each other

☐ Preventing runs on banks

☐ Preventing the value of the dollar from being artificially impacted compared to other currencies

Which of these components of the ***integrity of monetary and financial data*** does the infrastructure sector perform?

☐ Preventing monetary and financial data from being destroyed

☐ Ensuring the accuracy of banks' records of holdings

☐ Ensuring individuals' personal information is not maliciously altered

☐ Ensuring banks' customer data is not altered

☐ Maintaining accuracy of data relating to exchanges and stock markets

Which of these components of the ***security, flow, and integrity of goods and services through international trade*** does the infrastructure sector perform?

☐ Functionality of oil and gas pipelines

☐ Preventing the malicious disruption of supply chain management systems

☐ Preventing the disruption of sea transportation

☐ Preventing the disruption of land transportation

■ ☐ Preventing the disruption of air transportation

Which of these components of the ***security, flow, and integrity of goods and services through inter-state trade*** does the infrastructure sector perform?

☐ Functionality of oil and gas pipelines

☐ Preventing the malicious disruption of supply chain management systems

☐ Preventing the disruption of sea transportation

☐ Preventing the disruption of land transportation

☐ Preventing the disruption of air transportation

If Public Safety was checked:

What key missions of public safety do the infrastructure sector affect/perform?

☐ Disease outbreak prevention and mitigation

☐ Timely emergency services

☐ State and local law enforcement presence/response

☐ Access to basic needs

For those checked:

Which of these components of ***disease outbreak prevention and mitigation*** does the infrastructure sector perform?

☐ Dissemination of necessary medicinal supplies cannot be disseminated among the population.

☐ Identifying and, if needed, quarantining infected individuals

☐ Communication of necessary preventative measures to general public

☐ Communication of general population with public health authorities

☐ Ensuring access to patient records

Which of these components of ***timely emergency services*** does the infrastructure sector perform?

☐ *Notification of an incident to* emergency responders

☐ Access of emergency responders to affected area

☐ Access adequate supplies and equipment for emergency responders

☐ Transportation by emergency responders cannot of victims

☐ Communication between emergency responder elements

Which of these components of ***state/local law enforcement presence and response*** does the infrastructure sector perform?

☐ Communication and assessment of alerts from general population of criminal activity

☐ Communication between law enforcement elements

☐ Access to affected area

☐ Physically apprehension of perpetrators

☐ Incarceration of perpetrators

Which of these components of ***access to basic needs*** does the infrastructure sector perform?

☐ General population access to clean water.

☐ General population having shelter against adverse weather.

☐ General population access to a safe air supply.

☐ General population protection from adverse radiological or chemical elements.

☐ General population protection from unsafe structures or environments that threaten physical harm

---

Complete the following for each component checked underneath the red headings.

Key mission: __Preventing the disruption of air transportation (inter-state)_____

Component: __ground control_____

Does the component currently depend on cyber assets? (Y) N

If YES:

Is there a human or mechanical backup to adequately and quickly replace the functions of the cyber assets? (Y) N

If NO:

Should the component be lost due to destruction or manipulation of cyber assets, how many people would experience **loss of life**?

>10,000 | 1,000 - 10,000 | 100-1,000 | 50-100 | <50 | None

Should the component be lost due to destruction or manipulation of cyber assets, how many people would experience **severe injuries/illness**?

>10,000 | 1,000 - 10,000 | 100-1,000 | 50-100 | <50 | None

Should the component be lost due to destruction or manipulation of cyber assets, how many people would experience **minor injuries/illness**?

>10,000 | 1,000 - 10,000 | 100-1,000 | 50-100 | <50 | None

Should the component be lost due to destruction or manipulation of cyber assets, how many people would experience **inconvenience**?

>10,000 | 1,000 - 10,000 | 100-1,000 | 50-100 | <50 | None

What is the estimated recovery time of the cyber assets?

Years Months Days Hours Minutes Seconds

What is the estimated time length of the immediate, primary effects upon [national security, economic security, or public safety]?

Years Months Days Hours Minutes Seconds

Complete the following for each component checked underneath the red headings.

Key mission: __Preventing the disruption of air transportation (international)_____

Component: __ground control_____

Does the component currently depend on cyber assets? (Y) N

If YES:

Is there a human or mechanical backup to adequately and quickly replace the functions of the cyber assets? (Y) N

If NO:

Should the component be lost due to destruction or manipulation of cyber assets, how many people would experience **loss of life**?

>10,000 | 1,000 - 10,000 | 100-1,000 | 50-100 | <50 | None

Should the component be lost due to destruction or manipulation of cyber assets, how many people would experience **severe injuries/illness**?

>10,000 | 1,000 - 10,000 | 100-1,000 | 50-100 | <50 | None

Should the component be lost due to destruction or manipulation of cyber assets, how many people would experience **minor injuries/illness**?

>10,000 | 1,000 - 10,000 | 100-1,000 | 50-100 | <50 | None

Should the component be lost due to destruction or manipulation of cyber assets, how many people would experience **inconvenience**?

>10,000 | 1,000 - 10,000 | 100-1,000 | 50-100 | <50 | None

What is the estimated recovery time of the cyber assets?

Years | Months | Days | Hours | Minutes | Seconds

What is the estimated time length of the immediate, primary effects upon [national security,

economic security, or public safety]?

Years Months Days Hours Minutes Seconds

Possible Improvements

1) Do not make the user, the survey-taker, decide blindly at the on-set between national security, economic security, and public safety. Instead, have them answer the national security questions. IF anything is checked, then they continue with NS follow-up questions along the path that is relevant before proceeding with economic security questions. If nothing is checked for the initial national security question, the user would have continued straight to the initial economic security question. Upon arrival at that initial economic security question, they, again, either proceed with relevant ES questions or proceed to those designated for public safety.

2) Instead of presenting the survey-taker with an accompanying sheet of NS, ES, and PS definitions (or instead of solely presenting the user with these), the survey-*giver* should also supply the user with examples of the segmented, or topically broken-down portions, of each definition. These could serve as definitions themselves, guiding the user as they determine how their sector performs or supports the functions of NS, ES, and PS.

3) This process should begin by reviewing the definition itself, perhaps by peer review. This revision should purpose to elevate the scrutiny given to the definition by ensuring that each part of it combines to produce a comprehensive panorama of the security/safety indicator. The methodology presented could also benefit from reexamination to ensure that each component is appropriately included.

> These changes to the methodology presented here require additional research and present some architectural /methodological challenges. Both factors require additional time and resources that were not available to this group. Refining the segments of our definitions should resolve this potential weakness through a variety of means. Aside from intensified academic rigor behind the component selection process, one might consider experimenting by testing multiple and varied audiences for comprehension of questions. Simultaneously, one could survey the test audiences for feedback regarding comprehensiveness of basic indicator definitions. These efforts strengthen the utility of providing examples of reasons one might check a box, claiming their sector plays a role in certain duties associated with a given indicator. Furthermore, these measures would also ensure that examples listed prove helpfully descriptive, distinct, and unique to that component when possible. These changes should show that when taken as a whole, the list of examples is exhaustive/all encompassing of that component without being confusing, repetitive, or attention-challenging.

These enumerated improvements provide three major benefits. When this approach is employed and clarified by examples, the methodology then eliminates much of the ambiguity and confusion possible if the methodology is left in the current state. First, this change produces more generalizable results as the window of subjectivity closes. Second, this alteration further minimizes room for inflating the importance of a sector by stretching justification for choice selection beyond reasonable applicability. Third, the burden of proof is somewhat lifted from the survey-taker, as the examples lend clarity to the content of each element comprising the definitions (which we used as questions searching for mission relevance). The more user-friendly a tool is, the more useful it becomes as responses reflect more accurately and people more readily employ the tool.

4) As a further modification to this methodology, one might consider reversing the weighting logic applied in this questionnaire/program. The basic requirements for performing a function or supporting a mission should be weighted as the first step in an exponential climb. Those functions checked that require other functions as prerequisites should reflect the advanced nature of the mission with a higher ranking. Instead of the basic indicators carrying a value of three and those indicators that perform additional duties, or contribute to the indicator on a larger scale, carrying a value of one, the basics should receive a value of one and those duties requiring more resources and carrying a larger share of the burden should receive a value of three.

    Not only is this a logical and consistent way to weight options, but it produces greater variance in the results for those sectors that contribute in a broader sense or by more advanced means than for those which only contribute in a rudimentary fashion. This approach to weighting enables clearer comparative distinction, the more engaged a sector becomes in the key indicators core functions or missions.

5) One should also consider further developing the weighting system to accommodate situations wherein a user might have multiple reasons for checking one box. In other words, a sector might play a large role in only one area or function that can be checked. Perhaps this situation should produce a numerical value reflecting that this sector stands in contrast to another that might play only a small role but in more than one function.

    Inconsistently, every screen or question was not weighted in accordance with which functions serve as prerequisites for the next. For those occasions that this type of ordering system does not apply, another systematic approach is both lacking and needed. The above suggestion

captures the importance of a sector's role as it fits into the broader, more complete picture. It also provides opportunity for greater distinction in the impact, reflected in the comparative final value produced for each sector's involvement in each of the indicators, NS, ES, and PS.

This suggestion is not without its own obstacles to overcome before this can serve as a viable weighting method. An attempt to incorporate each and every way a sector contributes to each function of our indicators reintroduces opportunity for exaggeration and speculation. Unless these opportunities can be minimized, this approach pairs a step forward with a couple steps backward. The other problem that recurs by further complicating the system is that this change reintroduces the issue of time and energy-intensive scrutiny. These are additional resurfacing problems that counter-act earlier efforts to minimize subjectivity and make the survey easier for the user to take. Both factors were previously identified as important for meaningful, generalizable results needed when making important decisions like resource allocation.

6) Without reservation, the test administrator should use the results of the tool presented here in concert with other existing methodologies which specialize in separate but relevant data, like threats and vulnerability assessments. The tools collectively present a more complete and verifiable (in some cases) picture, assimilating all information useful for making decisions on where to allocate cyber-protecting resources that will maximize national security, economic security, and public safety.

Although some of the preceding recommendations are conditioned by overcoming certain problems and require further research to determine if and how exactly, this paper sets forth this recommendation for use of this survey/program in its present state. This methodology focuses on a comparative measure of a sector's involvement in national security, economic security, and public safety. Resource allocators will benefit by this knowledge in concert with risk assessments that reveal potential threats to and vulnerabilities within each sector. Using a risk assessment such as that found in *Physical Security…* , decision-makers can not only decide which sectors require what amount of protective resources, but they can also decide to what ends exactly the funds should contribute.

Bibliography

A Comparison of Oil and Gas Segment Cyber Security Standards (2004). http://www.us-cert.gov/control_systems/pdf/oil_gas1104.pdf

A Military Guide to Terrorism in the Twenty-First Century. US Army Training and Doctrine Command, Fort Leavenworth: US Army, 2006.

Adam, Nabil. “Workshop on Future Directions in Cyber-Physical Systems Security”. Department of Homeland Security. January 2010. http://www.ee.washington.edu/faculty/radha/dhs_cps.pdf

Ambassador (ret.) Napper, Larry. Professor and Director of the Scowcroft Institute, Bush School of Government and Public Service. College Station, TX. Interview. 2 February 2011.

American Petroleum Institute. “Industry Sectors”. March 31, 2011. http://www.api.org/aboutoilgas/sectors/index.cfm

Ayyub, M. McGill, W., and Kaminskiy, M. (2007) “Critical Asset and Portfolio Risk Analysis An All-Hazards Framework”. Risk Analysis, Volume 27, Issue 4, Pp 789-801.

“Backgrounder on Cyber Security.” Nuclear Regulatory Commission, 1 Apr 2010. Retrieved 14 Apr 2011. http://www.nrc.gov/reading-rm/doc-collections/fact-sheets/cyber-security-bg.html
Banking and Finance Sector: Critical Infrastructure and Key Resources. 29 December 2008.

Department of Homeland Security. 28 February 2011. http://www.dhs.gov/files/programs/gc_1188566544964.shtm

Bates, Theunis. “Scores Killed in Indian Train Crash.” AOL News. 19 July 2010. 5 Mar. 2011. http://www.aolnews.com/2010/07/19/scores-killed-in-indian-train-crash-sabotage-probed/

Benouar, Djillali. "Natural Hazards Threats to Critical Infrastructure in Algeria." 1st Annual Conference of the International Society for Integrated Disaster Management. (September 2009).
Brunner, Elgin M., and Manuel Suter. "International CIIP Handbook 2008/2009: An Inventory of 25 National and 7 International Critical Information Infrastructure Protection Policies." Center for Security Studies, ETH Zurich. (2009).

Butschli, Jim. "USPS Ups Efficiency with 'Smart' Conveyor Controls." Packaging World, 1997: 1.
Canada. National Strategy for Critical Infrastructure. 2009.

Carlson, R.E., J. E. Dagle, S. A. Shamsuddin, and R. P. Evans. “A Summary of Control System Security Standards Activities in the Energy Sector.” DOE Office of Electricity Delivery and Energy Reliability, October 2005.

Chen, Ping, Scown, Corinne, Matthews, Scott, Garrett, James and Hendrickson, Chris. (2009) “Managing Critical Infrastructure Interdependence through Economic Input-Output Methods.” Journal of Infrastructure Systems, Volume 15, Issue 3.

Chiappinelli, Chris. “Cyber-attack Threatens Manufacturing Software Systems Worldwide.” Managing Automation. Managing Automation, 22 Jul 2010. 22 Mar 2011. http://www.managingautomation.com/maonline/news/read/Cyber_attack_Threatens_Manufacturing_Software_Systems_Worldwide_33612

Cohen, Fred. “What makes critical infrastructures Critical?” International Journal of Critical Infrastructure Protection 2010: 53-4.

Comments on the Economic and Security Implications Of Recent Developments in the World Oil Market, 107th Cong. (2000) (testimony of Robert E. Ebel). http://hsgac.senate.gov/032400_ebel.htm

Commonwealth of Australia. Critical Infrastructure Resilience Strategy. 2010.

“Control Systems Cyber Security for the Natural Gas Pipeline Industry”. INGAA. January 31, 2011. http://www.aga.org/our-issues/security/Documents/INGAAControlSysCyberSecGuidelinesREV.pdf

"Control Systems Security Program." US CERT: Control Systems. http://www.us-cert.gov/control_systems/csvuls.html (accessed March 2, 2011).

Cordesman, Anthony and Justin Cordesman. “Cyber-Threats, Information Warfare, and Critical Infrastructure Protection.” Praeger Publishers: Westport, CT. 2002.

Corzine, Larry M. “Communication Breakdown: DHS Operations During a Cyber Attack.” Naval Postgraduate School Thesis Dec. 2010.

"CyberIntelligence Division Works Across Borders." Postal Inspection Service News, 2008: 2.

“Cybersecurity: Continued Attention is Needed to Protect Federal Information Systems from Evolving Threats.” Statement of Gregory C. Wilhusen, Director, Information Security Issues. Government Accountability Office. 16 June 2010. http://www.gao.gov/new.items/d10834t.pdf

"Cyber Security Guidance." https://www.fema.gov/pdf/government/grant/hsgp/fy09_hsgp_cyber.pdf (accessed February 27, 2011).

Dalson, Hal, Enrique Matheu, Yazmin Seda-Sanabria, Andres Lopez-Esquerra, and Kristen Baumgartner. “Addressing Cybersecurity Issues for Dams.” N.p., n.d. 13 Apr 2011. http://ussdams.com/proceedings/2010Proc/493-504.pdf

“Defense Industrial Base: Critical Infrastructure and Key Resources Sector-Specific Plan as input to the National Infrastructure Protection Plan.” Department of Homeland Security. May 2007: 4.

Deparment of Energy. “Transmission, Distribution and Storage”. 23, January 2009. http://www.fossil.energy.gov/programs/oilgas/delivery/index.html

DiBiasi, Jeffery R. “Cyberterrorism: Cyber Prevention vs. Cyber Recovery.” Naval Postgraduate School Thesis Dec. 2007.

Dobson, I., Carreras, B., and Newman, D. (2003) "A probabilistic loading-dependent model of cascading failure and possible implications for blackouts," Hawaii International Conference on System Sciences.

Dobson, I., Carreas, B., Newman, D., and Poole, A. (2004) “Evidence for self-organized criticality in a time series of electric power system blackouts”. Circuits and Systems I: Regular Papers, IEEE. Volume 51, Issue 9. Pp 1733-1740.
Dunn-Cavelty, Myriam and Manuel Suter. “Public-Private Partnerships are no silver bullet: An expanded governance model for Critical Infrastructure Protection.” International Journal of Critical Infrastructure Protection 2009: 179-187.

“Enterprise Software.” Capterra. 2010.
http://www.capterra.com/enterprise_software_definition
Espiritu, Jose, David W. Coit, and Upyukt Prakash. “Component criticality importance measures for the power industry.” Electric Power Systems Research No. 77, 2007: 407-420.

Fabro, Mark and Trent Nelson. “Control Systems Cyber Security: Defense-In Depth Strategies.” Idaho National Laboratory Publication. Oct. 2007.

FDIC: Dynamic Depositor Discipline in U.S. Banks. Federal Deposit Insurance Corporation. 12 April 2011.
http://www.fdic.gov/bank/analytical/working/wp2003_07/index.html#fig04

Fink, Raymond K., David F. Spencer, Rita A. Wells. “Lessons Learned From Cyber Security Assessments of SCADA and Energy Management Systems.” Idaho National Laboratory Publication. Oct. 2006.

Franchina, L., Carbonelli, M., Grat, L. Claudio, P. and Perucchini, D. (2009) . “An Effective Approach for Cascading Effects Prevision in Critical Infrastructures”. Critical Information Infrastructure Security. Berlin: Springer-Verlag.

"Flight Delay Information - Air Traffic Control System Command Center." Flight Delay Information - Air Traffic Control System Command Center. 05 Mar. 2011. http://www.fly.faa.gov/flyfaa/usmap.jsp

Folga, Steve, Timothy Allison, James P. Peerenboom, John Carr, Enrique Matheu, Yazmin Seda-Sanabria. "Incorporating Critical Infrastructure Interdependencies into Dam Failure Consequence Assessments." Critical Infrastructure Interdependencies 505-518.

Franchina, Luisa, Marco Carbonelli, Laura Gratta, Maria Crisci, and Daniele Perucchini. "An impact-based approach for the analysis of cascading effects in critical infrastructures." International Journal of Critical Infrastructures Vol. 7, No. 1, 2011: 73 – 90

FRB: Federal Reserve Districts and Banks. The Federal Reserve System. 12 April 2011. http://www.federalreserve.gov/otherfrb.htm

Garcia, Mary Lynn. The Design and Evaluation of Physical Protective Systems, Boston: Butterworth-Heinemann, 2008

Gewirtz, David. "How Critical Infrastructure is at Risk of a Cyber Attack." Journal of Counterterrorism and Homeland Security International Summer 2009.

Haimes, Y. (2005) "Infrastructure Interdependencies and Homeland Security". Journal of Infrastructure Systems. Volume 11, Issue 2. Pp 65-66

Haimes, Yacov Y., and Clyde G. Chittester. "A Roadmap for Quantifying the Efficacy of Risk Management of Information Security and Interdependent SCADA Systems." Journal of Homeland Security and Emergency Management 2.2 (2005). https://www.webdepot.umontreal.ca/Usagers/langlost/MonDepotPublic/infrastructures/Risk%20SCADA%20Systems.pdf

"Hacker Attacks Targeting Healthcare Organizations Doubled in the 4th Quarter of 2009 according to Dell SecureWorks' Data." Dell Secureworks. Dell, 26 Jan 2010. 27 Feb 2011. <http://www.secureworks.com/media/press_releases/20100126-healthcare-attacks/>.

Halbgewachs, R. "Control Systems Security Standards Accomplishments & Impacts" Tech. Rep. SAND2007-7019, Sandia National Laboratories, November 2007.

Hare, Forrest, and Jonathan Goldstein. "The interdependent security problem in the defense industrial base: An agent-based model on a social network." International Journal of Critical Infrastructure Protection. 3. (2010): 131.

"Health IT." The Office of the National Coordinator for Health Information Technology. Department of Health Services, 28 Feb 2011. 27 Feb 2011. http://healthit.hhs.gov/portal/server.pt/community/healthit_hhs_gov__home/1204

Hemond, Yannick and Benoit Robert. "Evaluation of the consequences of road system failure on other critical infrastructures." International Journal of Critical Infrastructures Vol. 6, No. 1. 2010.

Hurst; Flowers, James. "I&C Update on Plant Vogtle Units 3 and 4." POWER Magazine (1 Feb 2011): Retrieved 14 Apr 2011. http://www.powermag.com/nuclear/3389.html

Hurst, Timothy. "Time to get serious about security." POWER Magazine (15 Apr 2008): Retrieved 14 Apr 2011. http://www.powermag.com/smart_grid/Time-to-get-serious-about-security_69.html

"Incident Definition." United States Computer Emergency Readiness Team. Department of Homeland Security, Retrieved 31 Jan 2011. <http://www.us-cert.gov/federal/incidentDefinition.html>.

"Infogram 39-07." FEMA: US Fire Administration. October 4, 2007. http://www.usfa.dhs.gov/fireservice/subjects/emr-isac/infograms/ig2007/39-07.shtm (accessed March 6, 2011).
Internet Emergency Preparedness. http://datatracker.ietf.org/wg/ieprep/charter/ (accessed March 4, 2011).

Interview with electricity industry experts, BTU. 28 February 2011.

Interview with a senior aviation official at Easterwood Airport, College Station, TX. 17 February 2011.

Interview (telephone) with senior official at the Federal Reserve Board, Washington, DC. 8 March 2011.

Jenelius, Erik, Jonas Westin, and Ake J. Homgren. "Critical infrastructure protection under imperfect attack perception." International Journal of Critical Infrastructure Protection No. 3, 2010: 16-26.

Johnson, Charles. "Guidance Specifying the Technologies and Methodologies." Covered Entities for Security Rule. Health and Human Services, n.d. Web. 25 Apr 2011. <http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/hitechrfi.pdf>.

Judy, Deborah. Audit Report: Modem Security of the_____. Number IS-AR-10-009, Office of Inspector General.

Kawano, Kegan. “Designing Critical Infrastructure Cyber Security Segmentation Architecture by Balancing Security with Reliability and Availability.” Lecture Notes. 2008.

Macaulay, T. (2008) “Assessing operational risk in the financial sector using interdependency metrics”. International Journal of Critical Infrastructure Protection. Volume 1. Pp 45-52.

Making the Nation Safer: the Role of Science and Technology in Countering Terrorism. Washington, D.C.: National Academy, 2002.

McGill, William L., Bilal M. Ayyub, and Mark Kaminskiy. “Risk Analysis for Critical Asset Protection.” Risk Analysis Vol. 27, No. 5, 2007.

“Maritime Transportation Security Act of 2002,” H.R. 107-295, 107th Cong. (2002) (enacted). Text available at: http://www.tsa.gov/assets/pdf/MTSA.pdf

Matishak, Martin. “Nation's Nuclear Power Plants Prepare for Cyber Attacks.” Global Security Newswire, Nuclear Threat Initiative (27 Aug 2010): Retrieved 14 Apr 2011. <http://gsn.nti.org/gsn/nw_20100827_1692.php>.

McBride, Michael. “Cyber-Attacks against Internet-Enabled Medical Devices are New Threat to Clinical Pathology Laboratories.” Dark Daily. Dark Daily, 16 Feb 2011. 7 Apr 2011. http://www.darkdaily.com/cyber-attacks-against-internet-enabled-medical-devices-are-new-threat-to-clinical-pathology-laboratories-215

“Medical, Industrial, and Academic Uses of Nuclear Materials.” Nuclear Regulatory Commission, 16 Sep 2009. Retrieved 13 Apr 2011. http://www.nrc.gov/materials/medical.html
Meserve, Jeanne. “‘Smart Grid’ may be vulnerable to hackers”. CNN. March 20, 2009. http://articles.cnn.com/2009-03-20/tech/smartgrid.vulnerability_1_smart-grid-power-grid-blackout?_s=PM:TECH

Multi-State Information Sharing and Analysis Center (MS-ISAC). 28 Apr. 2011. http://www.msisac.org/

“National Council of ISACs.” ISAC Council. http://www.isaccouncil.org/

“National Security | Define National Security at Dictionary.com.” Dictionary.com | Free Online Dictionary for English Definitions. 27 Mar. 2011. http://dictionary.reference.com/browse/national+security

“National Security.” Encarta Dictionary. Encarta Online, 2009. 27 Mar. 2011. http://encarta.msn.com/dictionary_1861696682/national_security.html

"National Security Interests - Definition of National Security Interests by the Free Online Dictionary, Thesaurus and Encyclopedia." Dictionary, Encyclopedia and Thesaurus - The Free Dictionary. 27 Mar. 2011. http://www.thefreedictionary.com/national security interests

"National Security Strategy." The White House, May 2010. Retrieved 20 Apr 2011. http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf

NCS | National Communications System. 28 Apr. 2011. http://www.ncs.gov/index.html
Nelson, Trent. "Control System Security Center Common Control System Vulnerability." Idaho National Laboratory and the Department of Homeland Security. Nov. 2005. http://www.us-cert.gov/control_systems/pdf/csvul1105.pdf

"OCTAVE Information." Security Risk Solutions, Inc. 28 Apr. 2011. http://www.securityrisksolutions.com/OCTAVE.htm

Olson, James. Lecturer, Bush School of Government and Public Service. College Station, TX. Interview. 22 February 2011.

"P910 Manifest Mailing System (MMS)." P900 Special Postage Payment Systems. http://pe.usps.com/archive0810/p910.htm (accessed March 3, 2011).

PeopleSoft Enterprise Applications. Oracle. 28 February 2011 http://www.oracle.com/us/products/applications/peoplesoft-enterprise/index.htm

Permann, May Robin and KennethRohde. "Cyber Assessment Methods for SCADA Security." Idaho National Laboratory Publication. Jun. 2005.

Power, Richard. Cyber Security in the Three Times: Past, Present, and Future. CERT 20th Anniversary Seminar Series. Pittsburgh, PA. 22 July 2008.

"Privacy Impact Assessment for the Use of Social Networking Interactions and Applications Communications/Outreach/Public Dialogue." U.S. Department of Homeland Security. 16 September 2010. http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_dhs_socialnetworkinginteractions.pdf

Proc. of Strategies & Technical Solutions for Economically Managing Risk in a Multi-Threat Environment, San Francisco, CA. 28 Apr. 2011. http://www.managing-scada-security-risks.com/4/agenda/23/agenda/

"Radioactive Waste." Nuclear Regulatory Commission, 7 Jan 2011. Retrieved 13 Apr 2011. http://www.nrc.gov/waste.html

Ralston, P., Graham, J., and Patel, S (2006) “Literature Review of Security and Risk assessment of SCADA and DCS Systems”. Intelligent Systems Research Laboratory: Techinical Report TR-ISRL-06-01.

Ralston, P.A.S., J.H. Graham, and J.L. Hieb. “Cyber-security risk assessment for SCADA and DCS networks.” ISA Transactions Vol. 46, 2007: 583-594.

“Report of the Defense Science Board Task Force on Mission Impact of Foreign Influence on DoD Software.” Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, Department of Defense. September 2007: 72.

“Research and Test Reactors.” Nuclear Regulatory Commission, 16 Mar 2011. Retrieved 13 Apr 2011. http://www.nrc.gov/reactors/non-power.html

“(Revised) Implementation Plan for Cyber Security Standards CIP-002-1 through CIP-009-1.” North American Electric Reliability Council. http://www.nerc.com/fileUploads/File/Standards/Revised_Implementation_Plan_CIP-002-009.pdf

Rinaldi, S. “Modeling and Simulating Critical Infrastructures and Interdependencies”. Proceedings of the 37th Hawaii International Conference on System Sciences.

Robles, John Robles and Min-kyu Choi. “Assessment of the Vulnerabilities of SCADA, Control Systems and Critical Infrastructure Systems.” International Journal of Grid and Distributed Computing Vol.2, No. 2. Jun. 2009.

Ryan Hutson. Manager, Entergy Corporation. Telephone Interview. 25 February 2011.
Salesses, Robert. “Defense Industrial Base Conference Overview & Objectives,” Office of the Secretary of Defense for Homeland Defense and Americas’ Security Affairs. 11 Apr 2007: slide 10.

SAP for Banking: Delivering Solutions for the Dynamic Financial Services Environment. SAP Global. 28 February 2011. http://www.sap.com/industries/ banking

Setola, R., De Porcellinis, S., Sforna, M. (2009) Critical infrastructure dependency assessment using the input-output inoperability model. International Journal of Critical Infrastructure Protection. Volume 2, Issue 4. Pp 170-178.

“Security Guideline for the Electricity Sector: Identifying Critical Cyber Assets”. NERC. 17 June 2010. http://www.nerc.com/fileUploads/File/Standards/Critcal%20Cyber%20Asset_approved%20by%20CIPCl%20and%20SC%20for%20Posting%20with%20CIP-002-1,%20CIP-002-2,%20CIP-002-3.pdf

“Source Material.” Nuclear Regulatory Commission, 12 Feb 2007. Retrieved 14 Apr 2011. http://www.nrc.gov/materials/srcmaterial.html

Spellman, Frank and Bieber, Revonna. Chemical Infrastructure Protection and Homeland Security. Lanham: The Rowman &Littlefield Publishing Group, Inc. 2009. 40-41.

Shankar Sastry. “Understanding the physical and economic consequences of attacks on control systems.” International Journal or Critical Infrastructure Protection No. 2, 2009: 73-83

Sternstein, Aliya. "Postal Service IG Examines Cyber Incident Data." Next Gov: Technology and the Business of Government. August 2010.

"Summary of the HIPAA Security Rule." Health Information Protection. Health and Human Services, n.d. Web. 25 Apr 2011. <http://www.hhs.gov/ocr/privacy/hipaa/understanding/srsummary.html>.

Swanson, Marianne and Elizabeth B. Lennon. “Security Self-Assessment Guide for Information Technology Systems.” National Institute of Standards and Technology Publication Sep. 2001.
Technology Assessment: Cyber Security for Critical Infrastructure Protection. General Accounting Office, 2004.

Telephone interview with senior official at the Federal Reserve Board, Washington, DC. 8 March 2011.

“The Center for SCADA Security.” Sandia National Laboratories: Securing a Peaceful and Free World through Technology. 28 Apr. 2011. http://www.sandia.gov/ccss/

The CORAS Method. 29 Apr. 2011. http://coras.sourceforge.net/

Theoharidou, M., Kotzanikolaou, P.,and Gritzalis, D. (2010) A multi-layer Criticality Assessment methodology based on interdependencies. Computers & Security. Volume 29, Issue 6. Pp 643-658.

Tieghi, Enzo M. “Integrating Electronic Security into the Control Systems Environment: differences
IT vs. Control Systems.”
http://www.isticom.it/documenti/evidenza/13_Enzo_M_Tieghi.pdf

Thomason, Ronald. “Role of the Maritime ISAC: Training, Drills, Exercises, and Resource
Allocation.” Small Vessel Security Threat Conference. Ronald W. Shane Center, Miami Beach, FL. 8-9 Feb. 2011. Lecture.

“Transportation,” Kyland. 2009. http://www.kyland.cn/applilist_818.html

United States American Water Works Association. Roadmap to Secure Control Systems in the Water Sector. 2008.

United States. Dams Sector Roadmap to Secure Control Systems. 2010. 13 Apr 2011. http://www.damsafety.org/media/Documents/Security/DamsSectorRoadmaptoSecureControlSystems2010.pdf

United States Department of Homeland Security. "Commercial Facilities Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan." (2010): 57.

United States of America. Department of Homeland Security. Office of Intelligence and Analysis/Directorate for Preparedness. (U//FOUO) Strategic Sector Assessment: The Terrorist Threat to the U.S. Commercial Passenger and Freight Rail System. Homeland Infrastructure Threat and Risk Analysis Center (HITRAC), 24 May 2006. 5 Mar. 2011. http://abcnews.go.com/images/WNT/terrorist_threat_us_rail_system.pdf

United States. Government Accountability Office. Critical Infrastructure Protection. Challenges and Efforts to Secure Control Systems. 2004.

United States. Joint Chiefs of Staff (JCS). Department of Defense Dictionary of Military and Associated Terms. Defense Technical Information Center, 8 Nov. 2010. 15 Mar. 2011. http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf

United States. National Infrastructure Protection Plan: Agriculture and Food Sector. , 2008. 17 Apr 2011. http://www.dhs.gov/xlibrary/assets/nipp_snapshot_agriculture.pdf

United States. National Infrastructure Protection Plan: Critical Manufacturing Sector. 2009.

United States. National Infrastructure Protection Plan: Dam Sector. , 2008. 13 Apr 2011. http://www.dhs.gov/xlibrary/assets/nipp_snapshot_dams.pdf

United States. "National Infrastructure Protection Plan." Department of Homeland Security, 2009: 109.

United States. "National Infrastructure Protection Plan: Emergency Services Sector." Department of Homeland Security. Accessed February 26, http://www.dhs.gov/nipp.

United States. National Infrastructure Protection Plan: National Monuments and Icons Sector. , 2008. 17 Apr 2011. http://www.dhs.gov/xlibrary/assets/nipp_snapshot_nationalmonuments.pdf

United States. "National Infrastructure Protection Plan: Nuclear Reactors, Materials, and Waste Sector." Department of Homeland Security. 14 Jan 2010. Retrieved 12 Apr 2011. http://www.dhs.gov/xlibrary/assets/nipp_snapshot_nuclear.pdf

United States of America. Department of Homeland Security. Office of Infrastructure Protection. National Infrastructure Protection Plan (NIPP) Sector Specific Plan (SSP): Transportation Systems. DHS, May 2007. 20 Feb. 2011. http://www.dhs.gov/xlibrary/assets/nipp-ssp-transportation.pdf

United States. White House. Office of the President of the United States. National Security Strategy. By Barack H. Obama. May 2010. 14 Mar. 2011. http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf

"US-CERT: Control Systems - Cyber Threat Source Descriptions." US-CERT: United States Computer Emergency Readiness Team. 29 Apr. 2011. http://www.us-cert.gov/control_systems/csthreats.html

"U.S. Nuclear Power Plants." Nuclear Energy Institute. Retrieved 12 Apr 2011. http://www.nei.org/resourcesandstats/nuclear_statistics/usnuclearpowerplants/
US-CERT (United States Computer Emergency Readiness Team) Control System Documents. US-CERT, 2006. http://www.us-cert.gov/control_systems/csdocuments.html

Utne, I.B., Hokstad, P. and Vatn, J. (2010) A method for risk modeling of interdependencies in critical infrastructure. Reliability Engineering and System Safety. Pp 671-678

"Virtualization and Cloud Technologies Add Complexity to Disaster Recovery Initiatives." Symantec 2011 SMB Disaster Preparedness Survey. Symantic, 22 Nov 2010. 22 Mar 2011. http://www.symantec.com/about/news/release/article.jsp?prid=20101122_01