Common Threats and Vulnerabilities of Critical Infrastructures

Rosslin John Robles[1] , Min-kyu Choi[1], Eun-suk Cho[1],
Seok-soo Kim[1], Gil-cheol Park[1], Jang-Hee Lee[2]

[1] Department of Multimedia Engineering,
Hannam University, Daejeon, Korea
[2]College of Business Administration,
Dongseo University, Busan, Korea
rosslin_john@yahoo.com, freeant7@naver.com, eunsukk@empal.com,
{sskim,gcpark}@hnu.kr, ceo@korea.ac.kr

Abstract. Critical Infrastructure (CI) is used by governments as a term to describe infrastructures, systems and assets that are essential for the society and economy. Critical Infrastructures are so vital that an incapacity or destruction of such infrastructure, system or assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters. [1] This Infrastructures, systems or assets must be improved; this paper presents the vulnerabilities and threats to Critical Infrastructure, and discusses possible solutions and recommendations regarding this threats and vulnerabilities.

Keywords: Critical Infrastructure Protection, Threats, Vulnerability, Critical Infrastructure

1 Introduction

Vulnerabilities and threats to Critical Infrastructures and other related risks have been recognized for a long time. But this issue gathers great concern when in 1997 the US Presidential Commission on Critical Infrastructure Protection submitted a report which highlighted the topic of critical infrastructures. [2] Critical Infrastructure is classified as a National Concern [3] because of its scope and its importance to the nation. Identification of the Critical Infrastructure may differ in any countries.

The US government identified 14 areas or Infrastructures that required protection from threats. This infrastructure is so important because they provide goods and services that have great contribution to the economy and national defense. The survivability, reliability and resiliency of the systems identified as critical infrastructure allow the people to maintain a sense of confidence in their country and themselves. The National Strategy for Homeland Security has identified these 14 areas as: Agriculture & Food, Water, Public Health, Emergency Services, Government, Defense Industrial Base, Information ands Telecommunications, Banking and Finance, Energy, Transportation, Chemical Industry ands Hazardous

Materials, Postal and Shipping, National monuments and icons, and Critical Manufacturing.

2 Critical Infrastructures

The term “infrastructure” was defined by The American Heritage Dictionary [4] as:

“The basic facilities, services, and installations needed for the functioning of a community or society, such as transportation and communications systems, water and power lines, and public institutions including schools, post offices, and prisons.”

The US President issued an Executive Order 13010 which states that “certain national infrastructures are so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States". [5] It is where the term "critical infrastructure" was highlighted. According to E.O. 13010, these critical infrastructures were: telecommunications; electrical power systems; gas and oil storage and transportation; banking and finance; transportation; water supply systems; emergency services (including medical, police, fire, and rescue) and continuity of government. Figure 1 shows the infrastructures that were commonly pointed out as “critical”.

Most of these so-called critical infrastructures nowadays are controlled by controlled systems, SCADA in particular. So if the SCADA will malfunction, it will cause debilitating impact to the community and society.

Fig 1. Critical Infrastructures and assets

3. Threats to Critical Infrastructure

Threats to critical infrastructures can be classified into 3 categories, natural threats, human-caused, and accidental or technical. Natural threats include weather problems in both hot and cold climates and also geological hazards like earthquakes, tsunamis,

land shifting and volcanic eruption. Natural threats like this could greatly affect CI specially the transportation sector. For example, in 1995 an earthquake in japan destroys many Japanese critical Infrastructures. The highway was damaged, the port of Kobe which is Japan's largest container shipping port. It also damaged chemical manufacturers and steel manufacturers. [6]

Human-caused threats are sometimes referred to as terrorism. This may include cyber attacks, rioting, product tampering, explosions and bombing. Accidental and technological threats include such issues as transportation accidents and failures, infrastructure failures and hazardous material accidents. [7]

4. Critical Infrastructure Vulnerabilities

Vulnerabilities are characteristics of an installation, system, asset, application, or its dependencies that could cause it to suffer a degradation or loss (incapacity to perform its designated function) as a result of having been subjected to a certain level of threat or hazard. An example of this is the geographical location. Most Critical Infrastructures are geographically concentrated. This means that the physical location of critical infrastructures and assets are in sufficient proximity to each other. This also means that they are vulnerable to disruption of the same, or successive regional events. [8] The following are examples of infrastructures that are geographically concentrated.

- Transportation — Over 33% of U.S. waterborne container shipments pass through the ports of Los Angeles and Long Beach.[9]
- Transportation — Over 37% of U.S. freight railcars pass through Illinois and Over 27% of freight railcars pass through Missouri.[10]
- Chemical Industry and Hazardous Materials (chlorine) — Over 38% of U.S. chlorine production is located in coastal Louisiana.[11]
- Public health and health care — 25% of U.S. pharmaceuticals are manufactured in San Juan Metropolitan Area, Puerto Rico.[12]
- Energy — 43% of U.S. oil refineries located along the Texas and Louisiana coasts.[13]

Most critical infrastructures nowadays are controlled by controlled systems. An example of this are the SCADA systems that control the Energy Generating and distributing infrastructure, the water systems and electricity systems and other major infrastructures. These systems are usually connected to the network, which makes it vulnerable to cyber attacks. An individual or an entity with malicious intent might disrupt the operation of the system by blocking delaying the flow of information through the control networks. They can also make unauthorized changes to programmed instructions in the PLC's, RTU's and DCS controllers. This may result to

malfunctioning of an infrastructure. People involved in controlling the infrastructures must be a professional that knows a lot about the system.

5. Effects of Critical Infrastructure Attacks

Critical Infrastructure Attacks can be direct or indirect. Direct effects would be stoppage or disruption of the functions of critical infrastructures or key assets through direct attack on a critical part, system or function. For example the 9/11 attack of the World Trade Center which contain other critical assets, can be considered a direct attack on Banking and Finance infrastructure.

Indirect effects of an attack are the disruption and problems that result from a reaction to attacks on other critical infrastructure. Attacks on one critical infrastructure have effects to other infrastructure. If the transportation infrastructure will be damaged, other infrastructure like postal and shipping, emergency services and other infrastructures will also be affected. The following diagram shows that various critical infrastructures depend on each other. This also shows that if one of these infrastructures will be attacked, other will also be affected.

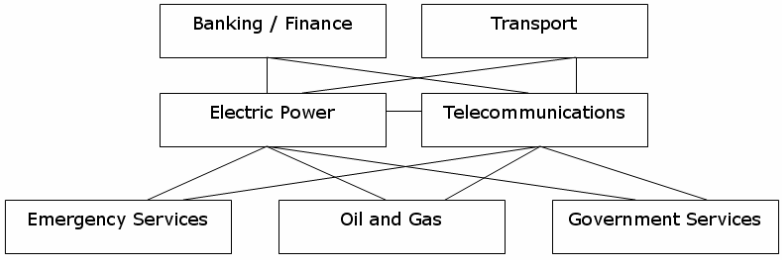

Fig. 2. Critical Infrastructure depending on each other [14]

Most systems in New Zealand assume the continuing supply of power and telecommunications. So if either of the power or telecommunications will be disrupted, many of the infrastructures will also suffer.

6. Critical Infrastructure Protection

It has always been the policy of the United States to ensure the continuity and security of the critical infrastructures that are essential to the minimum operations of our economy and government. This critical infrastructure includes essential government services, public health, law enforcement, emergency services, information and communications, banking and finance, energy, transportation, and water supply. Initially, critical infrastructure assurance was essentially a state and local concern. With the massive use of information technologies and their significant interdependencies it has become a national concern, with major implications for the

defense of our homeland and the economic security of the United States. However, given all of the focus on critical infrastructure still one in three critical infrastructure operations goes without a business continuity or continuity of operations plan and three out of five of those operations with plans have never tested their plans as "fit for purpose."[15]

Critical Information Infrastructure is perceived as an essential part of national security in numerous countries today and has become the nucleus of the US terrorism and homeland security debate after 11 September 2001. A critical infrastructure is commonly understood to be an infrastructure or asset the incapacitation or destruction of which would have a debilitating impact on the national security and the economic and social welfare of a nation. [16]

The Executive Order represents a clear political statement about the importance of Critical Infrastructure and Critical Information Infrastructure. It is important to understand that this is probably the clearest statement of this nature from any administration. It does, however, have a weakness in that there is a lack of absolute clarity on who is overall responsible – there is much coordination, different bodies, and consultation. No specific department is charged with either building resilience or defense, although it may be inferred that the Department of Homeland Security has a leading role

7. Recommendation

Critical Infrastructure can be protected by assessing the threats and vulnerability. After that, a plan to counter threats and vulnerabilities should be developed. Counter threats plan could minimize if not eliminate these threats and vulnerabilities. The following must be done to ensure Critical Infrastructure Protection:

1. Assess Critical Infrastructure vulnerabilities to cyber or physical attacks.
2. Develop plans to eliminate significant vulnerabilities.
3. Propose systems for identifying and preventing attempted major attacks.
4. Develop plans for alerting, containing and rebuffing attacks in progress.
5. Rapidly reconstitute minimum essential capabilities in the aftermath of an attack.

A security-organization should be established to provide timely information to critical infrastructure owners and government departments about threats, actual attacks and recovery techniques, build local capability in incident handling and security research, monitor global security issues and gather IT security intelligence, build relationships with similar organizations (e.g. CERT), promote cooperation among clients in respect of IT security, maintain statistics and incident, promote standards and tools for IT security and risk management, communicate to raise provider and public awareness of computer security issues, maintain a model security service level agreement for use in outsourcing arrangements, encourage production and adoption of relevant standards and facilitate independent security/protection audit capability.

8. Conclusion

Critical Infrastructures and assets are very important to a country because they contribute a lot to the society and the economy. These infrastructures must maintain their conditions in any circumstances. A lot of threats and vulnerabilities exist within and around these infrastructures. This paper discusses the threats that exist in Critical infrastructures. Critical Infrastructure vulnerabilities were also discussed and possible solutions to these problems. These infrastructures must be protected since they are so vital to the society and economy.

References

1. USA Patriot Act of 2001, incorporated into 2002 Act, from Interim National Infrastructure Protection Plan, Feb 2005
2. Y. Yurcik and D. Doss (2000) Information Security Educational Initiatives to Protect E-Commerce and Critical National Infrastructures
3. The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets (February 2003)
4. Andrew Hildick-Smith (2005) Security for Critical Infrastructure SCADA Systems
5. Wikipedia – SCADA http://en.wikipedia.org/wiki/SCADA Accessed: October 2008
6. Risk Management Solutions, Inc. 1995 Kobe Earthquake 10-year Retrospective. Newark, CA. (2005)
7. S. Snedaker (2007) Business Continuity and Disaster Recovery
8. P.W. Parfomak (2008) CRS Report for Congress "Vulnerability of Concentrated Critical Infrastructure: Background and Policy Options"
9. Army Corps of Engineers, Waterborne Commerce Statistics Center (WCSC). "U.S. Waterborne Container Traffic by Port/Waterway in 2006."
10. Assoc. of American Railroads. "Rail Carloads Carried by State: 2006."
11. U.S. Census Bureau, Alkalies and Chlorine Manufacturing: 2002
12. U.S. Census Bureau, Pharmaceutical Preparation Manufacturing: 2002
13. Energy Information Administration. Refinery Capacity 2008.
14. "New Zealand's Critical Infrastructure" http://www.e.govt.nz/archive/policy/trust-security/niip-report/chapter3.html#Toc501363185 accessed: October 2008
15. Kennedy, J (2006) Critical Infrastructure Protection is all about Operational Resilience and Continuity, Continuity http://www.continuitycentral.com/feature0413.htm Accessed: October 2008
16. Bush, GW (2001) Executive Order on Critical Infrastructure Protection. http://www.whitehouse.gov/news/releases/2001/10/20011016-12.html Accessed: October 2008