Int. J. Communications, Network and System Sciences, **2011, 4, 735-738**
doi:10.4236/ijcns.2011.411090 Published Online November 2011 (http://www.SciRP.org/journal/ijcns)

Computer-Based Infrastructure Sector Interdependencies and Security Implications

Aghware Fidelis Obukohwo
Computer Science Department, College of Education, Agbor,
Delta State, Nigeria
E-mail: *aghwarefo@yahoo.com*

Received August 17, 2011; *revised September* 21, 2011; *accepted September* 30, 2011

Abstract

Traditionally, the analysis of sector interdependencies has involved the characterization of all infrastructure-to-infrastructure interconnections and some of the main infrastructure integrals that, once lost or be tampered with, will compromise the performance and security issues with the other interconnected infrastructures. Therefore, the paper dwells much on the security implications which may be associated with these infrastructure sector interdependencies. This paper also discusses some of the major risk considerations, analytical approaches, researches and the necessary developments needed as well as the interdisciplinary ranges through which the necessary skills are required in the construction of comprehensive sector interdependencies.

Keywords: Infrastructure, Interdependencies, Sector, Security

1. Introduction

Interdependencies have always been done between connections which may be physical or virtual. In the field of computer science and technology, there have been increased interdependencies which integrate a number of infrastructures from different industries, both private and public in a way of increasing efficiency and improving the way of doing things [1]. There has been pervasive integration of computer resources and eventful automation of sector infrastructures, something that has been done over the last two decades. With these kinds of sectors, the infrastructure interdependencies are done through the application of informational, electronic links. This makes the output of one information infrastructure the input for another infrastructure in the interconnecttions, and what is passed across the interconnections is information which is the most valued commodity here. With this increase and extensive dependency on the sector interdependencies in some nations through the use of computer networks, most of the interdependencies have been vulnerable to any possible terrorist attacks. The problem here is due to the fact that the science applied in infrastructure interdependencies has not been developed as such and this is the reason why the systems are still vulnerable.

2. Literature Review

In 1990s, after successful recognition that computer resources could be effectively used in increasing the rate through which operations were done, it was necessary that there would be the integration of infrastructure sector interdependencies in all sectors [1]. Having done that, the issues of security became eminent and therefore the entire system could be easily compromised if necessary measure were not taken. This therefore calls for an analysis of the interdependencies in order to address all possible threats that would affect the systems. This analysis was motivated by the understanding and recognition that it would be possible to have a number of incidental infrastructures that could easily interact and therefore a single tamper with one point of the connections would bring the entire system to a halt. Again, any possible access of the system would also degrade the infrastructure sector interdependencies, therefore degrading the quality of service provided by the system. Having realized that the integration of these computer infrastructures was something delicate that could greatly bring bigger threats and risks once compromised, it was necessary to come up with ways and means through which the integrity of the system could be maintained. From the risk and threat point of view, any form of inter-sector analyses should be done in a manner that involves the characterization and identification of all the possible range of harms and threats that may exist to these infrastructure interdependencies [2]. Most of these threats will be posed by natural incidents, accidental occurrences, systems malfunctioning, or any form of intentional tampering. Some other form of threats may be from cyber or even physical damages. Some other misfortunes that may fall upon the sector interdependencies may be caused by what is known as loss consequences, and these may include issues to do with safety and health, economic issues, national insecurity, environmental interactions, and sociopolitical factors. Once it has been possible to understand the source and nature of the threat, then it would be possible to come up with an information foundation from which the system can be safeguarded through the use of defensible, cost-friendly mechanisms for protection. There will also be the incorporation of reliable decision support systems which are specifically for ensuring that there is security and sufficiency of the infrastructure sector interdependencies [3]. Since in the 1990s, the issue of security and system privacy is something that has been highly discussed with the sector interdependencies because there are very many possible threats which can be posed to the system, and end up bringing very many losses to the involved parties to that particular interdependency. Over the years, computer and software engineers have been coming together to give more findings and latest developments through which the issue of security can be addressed [4]. This has been done by looking at the past occurrences of threats and basing their research on that particular weakness point to ensure that it is not compromised again. These developments have been presenting the necessary advancements in the theory part, the system design, infrastructure implementation, the analysis, systems verification, and the evaluation for effective and secure infrastructure sector interdependencies. As we continue to have more and more smart computer devices each and every day, all the technological developments in the field of information and technology have undergone the change as well. On the other side, these systems and devices also become greatly compromised since there are more experts coming up with ways through which they can bring to a halt all the operations of the system [5]. Therefore, more and more research is needed in the field of computer technology in order to address the security implications and to increase our security technologies once some sectors are to adopt these infrastructure sector interdependencies. This will ensure that all the operations run smoothly and never will be compromised.

3. Infrastructure Sector Interdependence

Infrastructure maybe viewed as the fundamental building structures required for organizing an enterprise. It could also be seen as the technical frameworks, technologies and physical networks needed for the functionality of vital institutions in the society. Some basic examples include transportation, energy supply, water management, and communication.

3.1. Communication

In any nation, communications systems are the backbone for much of the critical infrastructure. It provides infor mation, such as data, video, and Internet connectivity, for other sectors in the national infrastructure. It provides information related to interdependent infrastructure from various government information systems, as well as information regarding the collaboration between government and the private sector. Interdependence is particularly relevant to the public safety community. For example, in the case of a power outage, public safety workers could lose access to critical resources, such as telephones and computers. Several recent large-scale power outages, such as the 2003 Northeast Region Blackout and Hurricane Katrina in 2005, have highlighted the strong interdependencies between the power and communications sectors. Such incidents emphasize the need for locally and independently generated power, which can provide electricity to public safety workers in times of emergency.

As important as they are, these systems and networks that make up these infrastructure are often taken for granted, yet a disruption to just one of those systems can have dire consequences across other sectors for instance, a computer virus that disrupts the distribution of natural gas across a region. This could lead to a consequential reduction in electrical power generation, which in turn leads to the forced shutdown of computerized controls and communications. Road traffic, air traffic, and rail transportation might then become affected. Emergency services might also be hampered. An entire region can become debilitated because some critical elements in the infrastructure become disabled through natural disaster. While potentially in contravention of the Geneva Conventions, military forces have also recognized that it can cripple an enemy’s ability to resist by attacking key elements of its civilian and military infrastructure.

3.2. Cyber Interdependency

Cyber interdependencies are relatively new and a result of the pervasive computerization and automation of infrastructures over the last decades. This interdependency is the one where Cuba has developed in the last 10 years the appropriate methods to cause damage to the United States.

Cyber interdependencies connect infrastructures to one another via electronic, informational links. The output of the information infrastructure are inputs to the other infrastructure, and the "commodity" passed between the infrastructures is information. Due to the extensive dependency of the nation's infrastructures in computer networks, this interdependency is the most vulnerable to terrorist attacks. The science of cyber infrastructure interdependencies is still relative immature and vulnerable. A deeper appreciation of its importance to national security has developed only in the last 10 years. Infrastructures are connected at multiple points such that a bi-directional relationship exists between the states of any given pair.

3.3. Security and Proprietary Data Issues

A highly detailed, comprehensive database of national infrastructures would be a valuable target for hackers, terrorists, and foreign intelligence services-particularly if it were coupled to advanced modeling and simulation. Some of the latest spies for Cuba had as a mission the development of such database. There is still the not completely solved case of the Moonlight Maze, an operation traced back to Moscow, by private engineers, and possible, not yet proven, with the assistance of Cuban engineers and computer scientists, in which unclassified DOD technology-related computer systems were compromised and sensitive data copied. This is the danger of creating of collecting data into one unclassified comprehensive database.

4. Security Implications

There can never be a greater threat than the issue of insecurity in a given infrastructure interdependency that had been initially adopted to improve efficiency and performance. This can bring about material losses, information loss, access of information by the wrong users, and so on. Different nations have adopted these interdependencies and the infrastructures are as well interconnected in way that makes them mutually dependent on each other in very many complexities. This kind of interconnection and interdependency is achieved through the use of information and communication technological advancements, also known as cyber-oriented computer systems [6]. Therefore, we will agree that any form of threat posed to the whole, or an integral part of the connection, will bring about the greatest worry. This means that whatever will happen at one end of a given infrastructure will directly impact the interdependent infrastructures in the entire system. This may as well affect very large geographical areas, and eventually halting the economic operations. At times, when there is an interconnection among a number of nations, the exact thing will also tend to happen. For instance, in the mid 1992, there was a failure with one of the telecommunications satellites in the United States, and this led to very huge inconveniencies as all pagers in the country malfunctioned. From the interdependency point of view, this brought a halt to a number of financial and banking operations in the country, affecting communication in hospitals and so one. As an example, any other form of interference in the system will therefore bring similar implications which may be harmful to any economy [6]. Having seen greater advancements in the global technology, it is true that any form of interruption and security threat posed on any infrastructure sector interdependencies will automatically give adverse effects on the running of the operations. Since more and more people continue to use the Internet, it becomes one of major points of interference through which an entire interconnection can be compromised. This will therefore bring greater losses to all the sectors linked to the interconnecttion. This will as well bring loss of vital information that may end up being used for social engineering and other cyber crime.

As it has happened over the years, a number of banking and financial institutions have been reported of having lost a lot of funds through cyber crime, and therefore gives us a hint on how this security implication can be something vital whenever thinking of infrastructure interdependencies. Therefore, any form of idea aimed at the identification, understanding, the analysis and monitoring of these interdependencies is something that should be done competently although this can be something quite challenging. This becomes the only sure way of safeguarding the existing interdependencies, and especially now that there have been increasing terrorism threats in different parts of the world [7]. It is very clear that all forms of computer based infrastructure sector interdependencies work through the support of a highly detailed, extensive and comprehensive data-source. This ensures that all information and decision support operations occur simultaneously in ensuring a smooth flow in the entire infrastructure connections [8]. The database holding these national infrastructures can thus become a very effective target for threats posed by terrorists, hackers, and some foreign intelligence operations, and especially when the data-base is coupled to a number of advanced simulations. Therefore, it would be necessary that all these issues are critically addressed whenever adopting a given infrastructure interdependency. There should also be means of ensuring that they are secure databases which hold different data so that the entire information and data is not located at only one access point.

5. Summary and Conclusions

Therefore, it will be the duty of the federal government to set up guidelines through which it can be easy to protect all critical sector infrastructure interdependencies. Since majority of these interdependencies are owned by the private sector, it would be necessary that there should be a guiding outline through which sector-based interdependencies will be adopted. It would also be necessary that all organizational interdependencies should be guided by appropriate modeling through which any loophole within the infrastructure can be tampered with, thus causing security issues. Also, it can be possible for all sectors in a given infrastructure interdependency to provide room for private-public sector interconnections so that they can jointly bring a cooperative environment in a way to protect all critical infrastructures. The sharing of these infrastructures will also ensure there is rapid economic growth since it would be easy to share information thus being able to solve any problem realized in the system immediately. Therefore, since security issues poses the greatest threat to any form of infrastructure sector interdependency, it would be necessary that everyone plays the role in ensuring that the entire system is safeguarded from any unauthorized access. There should also be the use of proper devices which may not be easily tempered for an effective operation of the entire infrastructure.

6. Recommendations

In an attempt to alleviate the menace on critical infrastructure sector interdependencies, the following steps need to be adopted:

- Sectors have to assess their vulnerabilities to both physical or cyber attacks;
- Plan to eliminate significant vulnerabilities;
- Develop systems to identify and prevent attempted attacks;
- A need to establish a center of excellence to support communities in conducting vulnerability and risk assessment;
- Application of information assurance techniques to computerized systems used by sectors such as water utilities, gas, and electric sectors, for operational data and control operations.

Alert, contain and rebuff attacks and then, with the Federal Emergency Management Agency (FEMA), to rebuild essential capabilities in the aftermath.

7. References

[1] J. Sullivant, “Strategies for Protecting National Critical Assets,” Wiley, New York, 2007. doi:10.1002/9780470228371

[2] J. Bullock and D. Haddow, “Introduction to Homeland Security,” New Jersey: Prentice Hall, Upper Saddle River, 2006.

[3] M. Amin “Toward Self-Healing Infrastructure Systems,” *IEEE Computer Application Power*, Vol. 33, No. 8, 2000, pp. 45-53.

[4] Y. Haimes, “Risk Modeling, Assessment, and Management,” John Wiley & Sons, New York, 1998.

[5] Y. Haimes and P. Jiang, “Leontief-Based Model of Risk in Complex Interconnected Infrastructures,” *Journal of Infrastructure Systems*, Vol. 7, No. 1, 2001, pp. 23-27. doi:10.1061/(ASCE)1076-0342(2001)7:1(1)

[6] S. Rosenbush, “Satellites’s Death Puts Millions out of Touch,” *USA Today*, May 1998. www.ieeexplore.ieee.org

[7] D. Verton, “Black Ice: The Invisible Threat of Cyberterrorism,” McGraw Hill, Upper Saddle River, 2003.

[8] J. Willenssen, “Critical Infrastructure Protection Signifycant Challenges in Safeguarding Interdependences,” Oxford University Press, Oxford, 2007.