Advances in Engineering Research (AER), volume 102
Second International Conference on
Mechanics, Materials and Structural Engineering (ICMMSE 2017)

Preventive measures for ICT critical infrastructure: A Review

R.T. Olorunfemi[1, a] and B.Twala[1]

[1]Department of Electrical and Electronic Engineering Science, University of Johannesburg, Auckland Park Kingsway campus, 2006, South Africa

[a]toppyrose6@gmail.com

Keywords: Computer network and attack, Critical infrastructures, Infrastructure protection, Information and Communication Technology, Information security.

Abstract. Critical infrastructures are very important tools which are paramount to the development of any nation. Therefore, they must be protected and catered for in order to promote their longevity. Information and Communication Technology (ICT) critical infrastructures are significant amenities which the nations depend solely upon in order to run their day to day transactions. Similarly, some advanced systems like the computerized integrated systems are used to support many functions and to improve their efficiency. Examples include the power grid generation control system, the railway stations in transport, the health infrastructure etc. There are numerous vulnerabilities and attacks on the network which these infrastructures are inter connected to in order to make them function well and to serve the populace. These attacks compromise the Confidentiality, Integrity and Availability (CIA) of a computer with internet network. However, this paper aims at providing comprehensive security gaps in ICT critical infrastructure and their preventive measures by critically reviewing related works that have been done and suggest possible ways to improving the system so that the people can be served well with the resources, and similarly to prevent the attackers from hacking into the system when there is a system breakdown.

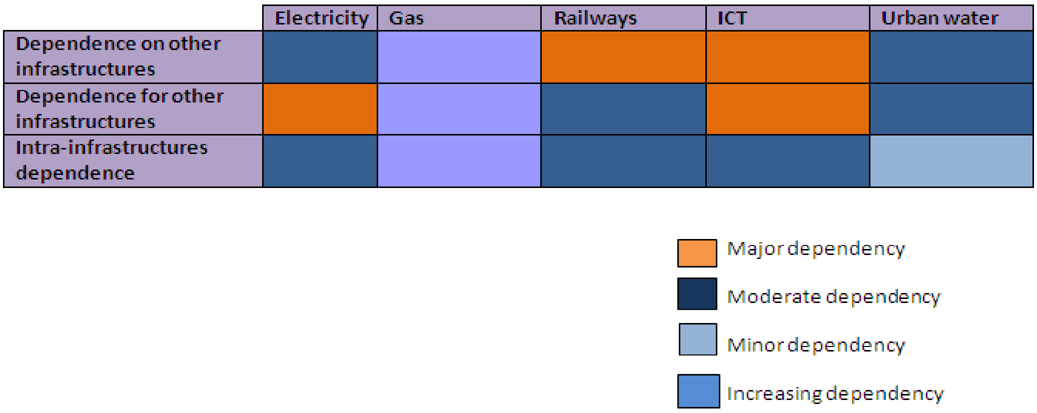
Introduction

Critical infrastructures (CI) are features and machines used by grassroots, national and the international community. Therefore, the incapacitation, breakdown or damage of any kind will bring an unbearable impact on all the social welfare of the general public. Large and complex critical infrastructures cannot be seen or categorized differently from Information and Communication Technology (ICT) because both are interwoven and thus, ICT is used to interconnect critical infrastructures with systems wired worldwide. Therefore, without ICT, the critical infrastructures cannot work properly to serve the populace. The ICT and CI are inter- dependent on each other which makes the infrastructures more vulnerable to attacks and this calls for urgent critical infrastructure's protection which depends solely on critical information infrastructure security [1].

Related Work

According to Wolfgang [2], the number of blackouts from August 2003 to November 2016 sits at 14 times ranging from different factors like human factors (wrong line security device setting, poor right-of-way maintenance, poor coordination among neighbouring countries) and technical factors such as high demand leading to overload and transformer fired damage to the main line as a result of construction work. His study proposed an object-oriented, hybrid approach combined with agent-based modeling techniques which can be employed to overcome a number of problems when compared to the conventional approaches being used to protect the infrastructures. Table 1 presents the inter-dependencies between five major infrastructures as indicated.

Table 1. Inter dependency between five major critical infrastructures [2].



	Electricity	Gas	Railways	ICT	Urban water
Dependence on other infrastructures	■	🟪	🟧	🟧	■
Dependence for other infrastructures	🟧	🟪	■	🟧	■
Intra-infrastructures dependence	■	🟪	■	■	□

🟧 Major dependency
■ Moderate dependency
□ Minor dependency
🟦 Increasing dependency

From the Table, it was observed that ICT has the major dependency on other infrastructure to function appropriately.

Also, in the research work of Schmitz [3] on the simulation and testing of instruments for critical infrastructures protection, the conventional methods of simulation was adopted in securing these infrastructures.

It was pointed out that securing critical infrastructures must be seen in a holistic approach by;

1. By securing the electronic security perimeter of the infrastructures.
2. By securing the network and lastly.
3. By securing the host environments.

Critical Infrastructure Problem

This section focuses on the challenges and issues relating to the critical infrastructure protection which can be subdivided as follows:

Information Security Problem. In any organization, the asset of that very organization is not only limited to the human beings, shareholders and buildings etc but also to the information security of the organization. The main core value asset of the organization is the data and information that go to and fro the systems and also archived in the computer systems of the organization. In the fore going, these resources need to be guided jealously and protected against any form of attack from either insiders or outsiders.

Insider Attackers. These are the attacks that occur from the employees that work in such an organization or institution. Such attacks can be caused directly or indirectly by the employees or indirectly in form of sabotage. It is therefore imperative to distinguish roles and privileges which an employee has to a particular information/ data that belong to the organization. A role/privilege assigned security system must be in place, where starting from the management of the organization to every employee is expected to have their roles and privileges outlined in a policy document and also be given the specified roles/privileges on the systems when they want to log in to the systems.

Outsider Attackers. This type of attackers collaborates with the insider in order to make their mission a successful one. The outsider attackers cannot carry out a clean and successful attack without some security breaches by the insider. This is the main reason why the insider attacker needs to be dealt with thoroughly in term of security wise; same goes to the outsider attackers. Although, the outsider attackers can perpetrate their evil even without the connivance of the insiders, but most times, they operate with the help of the insiders [4].

Solutions and Way Forward

This section details some proffered solutions and the way forward to critical infrastructures, and include the following:

Complex Critical Infrastructures. They depend solely on another critical infrastructure, and are firmly interconnected to each other in order for them to propagate and triumph from one critical infrastructure to another, and serve the populace effectively. Therefore, the operators must put this into consideration as part of the ethics when operating these infrastructures. They must also be operated with a holistic approach and not dependency; rather be interdependent on each other to function and serve the populace well [2].

Need for Public-Private Partnership. It is well known that, almost all the companies are privately owned by individual or joint, so there is a need for the private owners to go in agreement or partner with the government to make their infrastructures safe. However, a need for public-private crisis management will play a crucial role in critical infrastructure's protection. If this is achieved, it will help to build a resilient systems and providing training which could enhance security awareness programs etc.

Audit and Evaluation. Particularly for inter-organizational workforce, the audit team should be able to determine if the protections which are clearly defined in the security policy are being correctly adhered to in practice; logs on relations to partners, to verify if they comply with the previously signed contracts, and also provide evidence in case of disagreement or dynamic abuses should also be kept for variability.

Vulnerability and Risk Analysis. Vulnerability in this scenario regards to flaws and lapses that are in the system, that makes it easily susceptible to attack or damage as the case maybe. For example, in the system design of an application, some vulnerabilities can creep in through the coding process while in the power grid of power generating system, it can happen through human error or during installations of the components. Thus, in protecting our CI, all these factors must be taking into consideration in order to have a safe use. The risk analysis has been on use for decades now and it will continue to strive with the rate at which our networks are becoming more prone to attacks. Risk analysis can be defined as finding faults that might want to occur and quickly correcting them before they manifest, and as such a thorough scrutiny must apply to prevent such risk from manifesting [4].

User Education. It is widely been said that people are the weakest links in an attempt to secure the systems and the networks. It is of utmost importance to carry both the users and the operators along in the case of sensitization and awareness by providing trainings, workshops and seminars in information security to keep them abreast of the latest development as presented by Jose et al.[5]. According to Kim- kwang [4] in 2007, 'microsoft investigated attacks against Microsoft Word which was used as vulnerability in Microsoft Office 2000 and Office XP that allowed remote code execution whenever a user opened an infected document. There was an increasing awareness among the end-users of the call for fundamental security online, steady and continuing encouragement of a custom to cultivate a security consciousness for both the information systems and the networks among end-users. It is also important to make sure workers, and the public are carried alongside with other technology in order to control crime developments, and how the latest security measures can be of use to their advantage.

Considering the Term "Resilience". It is one of the major keys that must be taking into consideration in protecting CI. According to the Society for Risk Analysis (SRA)'s glossary, resilience van be define as the ability of a system to go back to its original or initial state of functionality after going through a major attack or a hazardous condition. Relating this definition to CI's resilience, it means the ability to witness internal drifts and cascading failure and still recover back to its initial operation condition [6].

Conclusion

Conclusively, critical infrastructures are complex systems in which small components are built together to form gigantic systems in order to serve the general public. Due to its interconnectivity and complex in nature, its security measures need to be viewed in a holistic approach from the top to the grass-root, ranging from the policy makers down to the smallest unit in an organization. All participating members need to see the security of these systems as a team work and not disintegrated as one person's work.

Also, a lot of researches have been conducted focusing on approaches, models, designs and simulations etc, and all of these must be taken into cognizance in order to have safe critical infrastructure with improved efficiencies.

References

[1] M. Theoharidou, D. Xidara and D. Gritzalis, A CBK for information security and critical information and communication infrastructure protection, Int. J. Crit. Infrastruct. Prot. 1 (2008) 81-96.

[2] W. Kröger, Critical infrastructures at risk: A need for a new conceptual approach and extended analytical tools, Reliab. Eng. Syst. Saf. 93 (2008) 1781-1787.

[3] W. Schmitz, Simulation and test: Instruments for Critical Infrastructure Protection (CIP), Inform. Secur. Tech. Rep. 12 (2007) 2-15.

[4] K. R. Choo, High tech criminal threats to the national information infrastructure, Inform. Secur. Tech. Rep. 15 (2010) 104-111.

[5] J. M. Yusta, G. J. Correa and R. Lacal-Arántegui, Methodologies and applications for critical infrastructure protection: State-of-the-art, Energy Policy, 39 (2011) 6100-6119.

[6] A. Lauge, J. Hernantes and J. M. Sarriegi, Critical infrastructure dependencies: A holistic, dynamic and quantitative approach, Int. J. Crit. Infrastruct. Prot. 8 (2015) 16-23.