INTERNATIONAL JOURNAL OF ACADEMIC RESEARCH IN BUSINESS & SOCIAL SCIENCES
HRMARS MANAGEMENT ACADEMIC RESEARCH SOCIETY EXPLORING INTELLECTUAL CAPITAL
www.hrmars.com
ISSN: 2222-6990

An Innovative Cyber Security based Approach for National Infrastructure Resiliency for Sultanate of Oman

Badar Mohammed Al Mughairi, Haitham Hilal Al Hajri, Asif Mahbub Karim, Mohammad Imtiaz Hossain

To Link this Article: http://dx.doi.org/10.6007/IJARBSS/v9-i3/5780 DOI: 10.6007/IJARBSS/v9-i3/5780

Received: *02 Feb 2019,* ***Revised:*** *19 Feb 2019,* ***Accepted:*** *29 Feb 2019*

Published Online: 12 March 2019

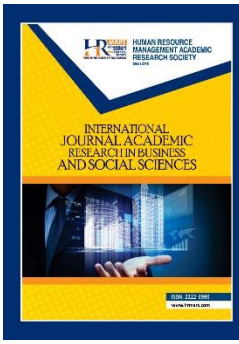
In-Text Citation: (Mughairi, Hajri, Karim, & Hossain, 2019)

To Cite this Article: Mughairi, B. M. Al, Hajri, H. H. Al, Karim, A. M., & Hossain, M. I. (2019). An Innovative Cyber Security based Approach for National Infrastructure Resiliency for Sultanate of Oman. *International Journal Academic Research Business and Social Sciences*, *9*(3), 1180–1195.

Vol. 9, No. 3, 2019, Pg. 1180 - 1195

http://hrmars.com/index.php/pages/detail/IJARBSS | **JOURNAL HOMEPAGE**

Full Terms & Conditions of access and use can be found at
http://hrmars.com/index.php/pages/detail/publication-ethics


INTERNATIONAL JOURNAL OF ACADEMIC RESEARCH IN BUSINESS & SOCIAL SCIENCES
HRMARS MANAGEMENT ACADEMIC RESEARCH SOCIETY EXPLORING INTELLECTUAL CAPITAL
www.hrmars.com
ISSN: 2222-6990

An Innovative Cyber Security based Approach for National Infrastructure Resiliency for Sultanate of Oman

Badar Mohammed Al Mughairi[1], Haitham Hilal Al Hajri[2], Prof. Dr. Asif Mahbub Karim[3], Mohammad Imtiaz Hossain[4]

[1,2]PhD Researcher, Binary University of Management & Entrepreneurship, Malaysia

[3]Dean, Binary Graduate School, Binary University of Management & Entrepreneurship, Malaysia

[4]MSc Scholar, Faculty of Economics and Management. University Putra Malaysia, Malaysia

Abstract

Critical National Infrastructure (CNI) within Oman is becoming Inter-independent to each other, aiming to provide unified and faultless services from the perspective of economics, quality, and governance. The new structure of interconnectivity between the CNI organizations has allowed sharing critical factors in benefiting from other CNI resources and services. Since this interconnectivity has permitted services and system to be more communicative and accessible via the internet, this has allowed some of the cyber threats to create a challenge to secure. Allowing such services to be available via the internet will also add to the fact that this services would be vulnerable to a variety of existing attacks.The latest global events related to Cyberterrorist attacks, have shown to the world how serious this matter.

In this article, we present a systematic approach after reviewing existing papers to building resilient cyber security networked systems. We first study fundamental elements of cyber security, cyberspace, CNI and its impact. Then we used qualitative methodology and case studies methods for better understanding the global incidents. This understanding drives the organizations of a distributed multilevel architecture that lets the network defend itself against, detect, and dynamically respond to upcoming challenges.

The recent attacks like operation petrol besides financial sector attacks in Oman shown the vulnerability of CNI system. In this case, we take the bank Muscat Visa attack as an example where they have announced that there visa credit card have been violated and a group of hackers compromised the system. To have better control and to handle on this matter, the management of such incidents should have been treated by a Cyber Center, who is well equipped and trained to

handle this type of events. This paper proposes an innovative Cyber Security based approach for National Infrastructure Resiliency for Sultanate of Oman which can be used as a framework of initiating National Cyber Security Centre aiming to monitor and control the CNI cyber threats and increase the awareness and readiness within the related organization based on many published article and study in this field. Finally, this paper opens the door to establish this type of center in the country in addition to offers future research directions to develop and implement a new and useful technique in the field.
Keywords: Critical National Infrastructures (CNIs), Interdependencies, Cyberterrorist attacks, Cyber Security, Oman

Introduction

This paper covers a topic which has limited consideration by the organizations or authority within the Sultanate of Oman, as there is no evidence of an article that supports this topic within the research filed, till the date of writing this Paper. The Critical National Infrastructures (CNIs) are organizations that play a very critical role upon the economy and the stability of the country (i.e., financial and living standards), which if exploited will have a significant impact to the government and may conclude to making these CNI's futile(Security, 2011).

The threats to the CNI Systems rely on technology in general. However other concerns and impacts may be a factor in the instability of the production of the CNI Systems. The Fact that, CNI systems linked with other industries make it crucial. Therefore the need to ensure the security of the CNI system has become an essential step (Cornish et al, 2011).

A recent study by SecurityScorecard, a company that provides organizations with security risk ratings, analyzed the security postures of 552 local, state, and federal government organizations. Across all industries surveyed including transportation, retail, healthcare and more, government organizations received one of the lowest security scores (Cyber security Report ,2017). Another report of The Gulf news (2017) regarding Information Technology Authority's (ITA) Annual Report 2017, provide evedence that Oman thwarted more than 880 million cyber attacks on government networks in 2017, according to the A total of 1.41 million attacks specifically targeting government websites were successfully warded off in 2017, compared to 1.75 million in 2016.Recently Oman have attacked by cyber terrorist that proves their exist space to improve their current system.Unfortunately,there have very limited research on cyberSecurity framework development in the Omani context.This article tries to fill the gap.

Moreover, this paper aims to create an innovative cyber security approach to identify and outline some of the persistence or existing Cybersecurity threats that targeting Critical National infrastructure (Communication Networks and Controllers) such as Power Energy sectors. Considering the proposed solution and countermeasure cannot cover all the vulnerabilities within the implemented solution or protect the industry from the targeted cyber threats('Computer Fraud & Security', 2001). For that, the collaboration and national monitoring firm for the national infrastructure come into the picture. The current issues that faced the IT Admins are the possibility of a security breach which could not be identified or monitored, even worse when they can spot the security breach but can't contain the issue.

Furthermore, some major infrastructure organizations become so big that they do not follow the security guidelines and that would result on more methods and way where hired hackers or cybercriminals may utilize to their benefit (Singh et al, 2014). Therefore the need to have innovative cyber security based approach for national infrastructure resiliency for Sultanate taking care of the incident controlling and handling is becoming a necessity, along with that the possibility of around the clock monitoring of Critical systems and networks becomes very important.

Critical National Infrastructure (CNI)

According to Chatham House 2003, The Critical National Infrastructure (CNI) is referred to individually as "Infrastructure assets" and as stated in the definition - may be physical (e.g. refinery sites, vital installations,) or logical e.g., information networks, systems, cyberspace (Cornish et al, 2011).

Critical National Infrastructure is a group of the organization's that functions within the country infrastructure, and they are considered as essential because the country's foundations are highly dependent on them. In addition to that if those organizations have affected its Confidentiality, Integrity, and availability (CIA) it would create a significant impact on the economic and security of the country(Choo ,2010). The below table illustrates the CNIs Sectors within the states which considered as a critical sector according to Oman National CERT (OCERT)(CERT Oman National, 2010).

Figure 1: CNIs Organization Type

The above-listed sectors included the Energy (Utilities), Oil and Gas (Supply and Processing), Financial services, Food (Production and Supply), Government, Emergency Service (Law enforcement / Defense Services), Health, Transport, Water (Utilities and Production), and Communications/ Telecommunications. Currently the critical infrastructures; government and private depending on the internet and online connectivity for everything and becoming connected with each other aiming to build connections and collaborative services (Bruijne & Eeten, 2007).The connectivity between organizations within and between the country/countries becomes essential to exchange information with similar services and similar/different sectors (Jang-Jaccard & Nepal, 2014)
This connectivity's introduce threats to the connected organization by having open environment and services that may target by the intruders that may get the CIA compromised. Furthermore, critical infrastructure that provides or sustain a sensitive role in the rise and development of the nation. Without this infrastructure, the country may fall and become nonfunctional, that may cause a severe impact on the economy or the stability of the country. For example; Water industry, electricity industry, health industry, food industry, transportation industry, communication industry all considered to be a CNI and they are the backbone of any healthy and stable nation, if these industries have a suffered from a malfunction, it will have a severe impact on the national stability.

Cyberspace

Cyberspace is a world that exists virtually where a group of nodes (computers) connected with each other globally to exchange data (Stevens, 2013). Therefore, its enable the data and services to be shared between the connected computers in many forms like TXT, Image, video or Code (Duroy, 2011). Cyberspace has revolved to a much larger purpose and needs; it has become a new way of life, cyberspace has become a necessity of life, where the whole globe are getting into cyberspace to carry a variety of activates. However, with the advanced technologies in hardware and software, it has made sharing knowledge over the virtual world an easy task.
Unfortunately, cyberspace has become an open arena, where the survivors are the elites who are using the most advanced technology or protection systems. Furthermore, the rising number of malware and hacking activates have skyrocketed insanely high compared to the situation 15 years ago.

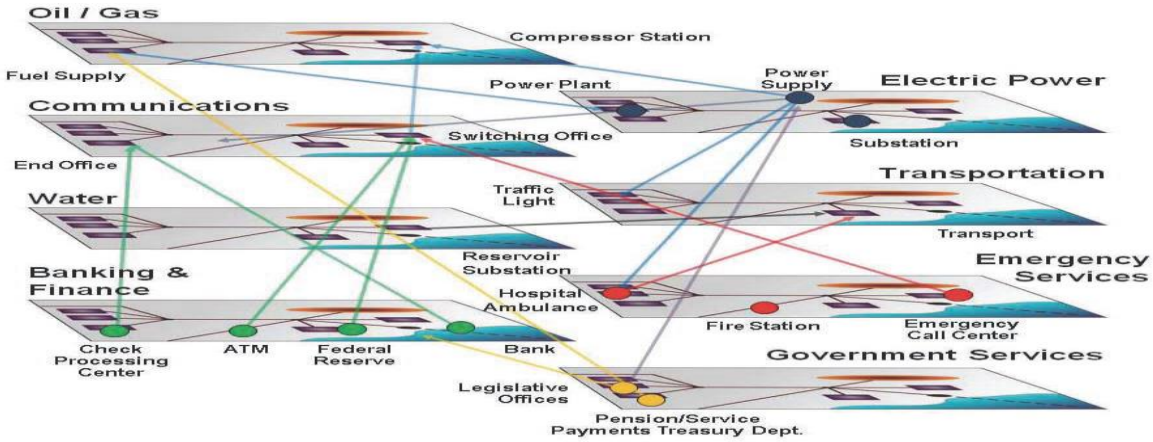
The needs of CNI to be connected to Cyberspace

CNI like any other industry requires monitor and controls. In addition to that, it used to be an isolated island where all controls are within the physical location. However, this trend has become a legacy method that no longer can be applied at the current time, because a modern infrastructure requires interconnectivity, such as remote accessibility that could be used for various reasons. The most basic and essential requirements would be the need for remote access for operation and administration purposes (Rinaldi, 2001). The current advanced technologies in hardware and software are built and designed to enable internetworking interaction, so it becomes remotely accessible and manageable in cases of emergency by authorized staff to overcome the persistence issues.

The ability to do so will save time and money because instead of traveling to the location that may take a long time but when it will be connected to the internet the cyber threats will be introduced to

such critical organization which may result on serve damage that will impact and risk its operation and functionality. In another hand, the facility may require some tweaks and updates on its functions in irregular bases. Sometimes it may need to be tested from overseas by its mother company. Occasionally the facility needs to be adjusted to best practice configuration based on the current requirements and needs. Therefore having the CNI connected to the GRID (cyberspace) has become a necessity that can not avoided. Therefore, CNI has moved from the typical isolated island to more advanced and connected hub which makes it more accessible consequently it has become more vulnerable (Yunos, 2010). The following diagram shows the example of conceptual Interconnections within and between Critical National Infrastructure.

Figure 2: Example of conceptual Interconnections within and between Critical National Infrastructure



Source: Foster et al, 2008

Cyber Threats to CNI

The United States Government Accountability Office 2012 states that the source of the threats that target the Critical Infrastructure can be generated from different sources as the below tables show(GAO, 2012):

Table 1: Cyber Threats Sources

Bot-network operators	Criminal groups
Hackers	Insiders
Nations	Phishers
Spyware or malware authors	Terrorists

Each one of the mentioned sources of the cyber-threats can conduct various methods or exploit (Attacks) which may affect the systems and services within Critical National Infrastructure which impact the operational and business activities within such organization. The following table lists the types of cyber exploit that can affect the CNI when it is connected to cyberspace(GAO, 2007):

Table 2: Types of Cyber Exploit

Denial of service (DOS)	Logic bomb	Exploit tools
Distributed Denial of Service (DDOS)	Sniffer	Trojan horse
Virus	Worm	Spyware
War-dialing	War-driving	Spamming
Phishing	Spoofing	Pharming
Botnet	Malware	

In addition to that, there are many published news and articles show that the Cyber Space and Information and Communication Technology (ICT) utilized to conduct some of the mentioned above cyber threats techniques and exploit targeting vulnerable organization and systems. The following are an example of such conducted cyber-attack that has been targeted a different type of organizations:

On 15 October 2013, Gavin Hill, the director of product marketing and threat research center published an article on SC magazine states that the apple application has a vulnerability which utilized by attacker to intercept the traffic between end-user who are using the IOS devices and Apple Store due to the sent traffic without encryption as plain text(Hill, 2013). The below graph illustrates the mentioned threats and vulnerability.

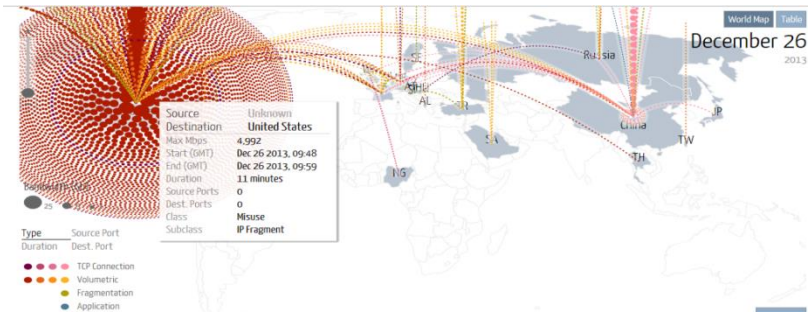
Figure 3: Exploitation Techniques of Apple Application Vulnerability

Source: (Hill,2013)

In 2008 the Russian hackers conducted Denial of Service attack targeted Georgian media which lead to bring down the service and make it unavailable and unreachable (Shakarian, 2013).

The Digital Attack Map which is a well-known website for monitoring DDOS Attack worldwide states that, the United State has been targeted by the DDOS attack on 26 December 2013. This attack has been conducted by different attackers from different countries as shown in the below DDOS attack Map(Map, 2013). According to Shakarian (2013) the DDOS attacks cost the banks 30,000 US Dollars for every minute their websites were down on 26 June 2013.

Figure 4: Digital Attack Map



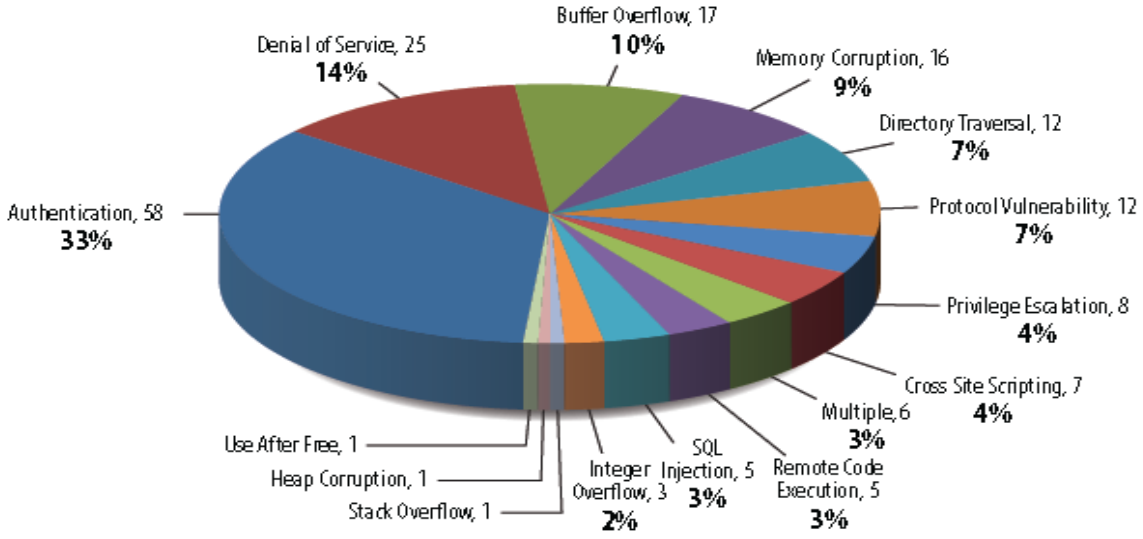
Source: (Map, 2013)

Existing Vulnerability within CNI

Vulnerabilities may exit within any installed Infrastructure, systems, applications or its dependencies that may affect the operations performance and functions of the infrastructure if it is subjected by any cyber threats. A report published by NSS Labs 2013 in regards to comprehensive analysis of vulnerability and threats within Critical National Infrastructures stats that, the security vulnerabilities in critical infrastructure escalated up 600% since 2010(Labs, 2013). Furthermore, the United States Computer Emergency Readiness Team declared that they had discovered 177 vulnerabilities within the infrastructure and systems used by different vendors in 2013 and the 87 percent of those vulnerabilities can be exploited remotely, and 13 percent need have access locally to conduct the exploitation(ICS-CERT 2014).

The above reports and statistics indicate that the cyberspace and connectivity can be threatened the functionality and operation of the running systems within the CNI by utilizing the existing vulnerability which may risk the organization. The below figure illustrates the different types of vulnerability according to ICS CERT which has been reported in 2013.

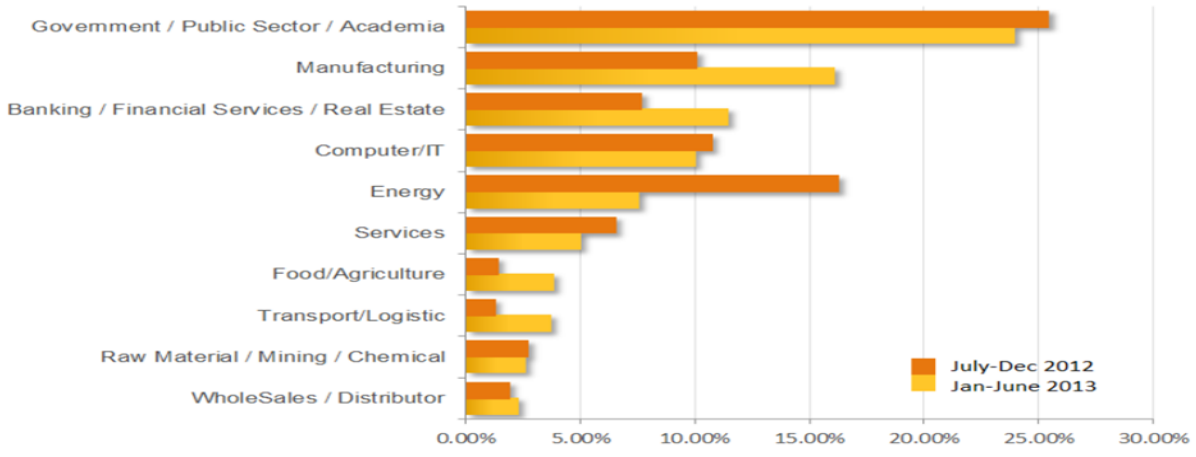
Figure 5: Different types of vulnerability according to ICS CERT



Source: Liang et al , 2017

The Symantec Security Response Report 2014 stated that the number of attacks or attempted attacks worldwide against national infrastructure is increasingly noticed, and it differs from sector to another. For example, the com arison between year 2012 and year 2013, the cyber-attack which targeted oil and gas sector increased from 7.6 % to 16.3 % compared with the power sector, as the reports illustrated the attacks on oil and gas sector increased significantly(Symantec, 2014). The below graph exemplifies the comparison attacks with different sectors between 2012 and 2013.

Figure 6: The comparison attacks with different sectors between 2012 and 2013



Source: (Wueest, 2014)

As per the illustration on the figure (6), it is noted that the government and public sector including academia were on the lead of the targeted sector. However, the manufacturing sector is considered

as the working force of the nation, and if it has been shut down by a successful attack it will cause a considerable loss, and in some cases, it may cripple the development of the nation or the national stability.

The chart list shows the finance sector along with real estate, as this is the proactive sector that depends on the backbone of finance and real estate is the third sector which has been targeted by the hackers, and it is very important for the nation to ensure its financial stability and won't be affected by the cyber-attacks.

The Impact of Cyber Threats to CNI

The impact of cyber threats based on Persistent advanced threats, which will be illustrated below:

Advanced Persistent CNI Malware Threats

TOP malicious malware known as Stuxnet, Duqu, Shamoon, and Flame is considered to be among the first and most advanced malware code that ever written. Security experts, have said that this specific malware has taken the game to a whole new level as the malware code used was so advanced that it had not been caught on the wild for a really long time. Some of the malware had used up to four Zero Day vulnerabilities aiming to ensure their ability to infect the targeted system (Bilge & Dumitras, 2012).

The rise of such new malware code has made a rumble on the ICT security world. The analysis of such code has revealed that the code is a not a product of one writer or a group of hackers, some explicated that this code has been build, engineered and funded by a group of governments, as the level of sophistication is above the ability of most hired hackers. In addition to that, the desired outcome is not something the average hacker would get himself into, the code analysis has revealed a clean and advanced way of coding only proves that this worked is done by experts who know what they are doing and know what they want. Furthermore, the expert said, the designed malware is so advanced that it could operate across highly secure networks, monitor and control everyday computer functions to send secrets and data to its command and control centers also known as CNC. The Malware could activate computer services such as microphones and cameras, log keyboard strokes, take screenshots, extract geographic location data from images, and can send all that using Bluetooth wireless technology(Nakashima, 2012).

Case Study

Information security researchers illustrate that there is more than four malware code which has significantly advanced programming code. This malware can even though they may be perceived as targets. However, it was detected to a specific function. Evidently, the Stuxnet and flame targeted nuclear reactor controls, where Duqu and Shammon targeted oil and gas industry, overall all the attacks targeted CNI Industry, and this can be considered as an example of cyberwar.

Stuxnet (Iran) Stuxnet (Iran)

The Stuxnet malware considered as the first malware targeted and threaten the Industrial Control System that used within the Critical Infrastructure such as pipeline and power planet (Shakarian, 2013). In 2010 the Stuxnet malware targeted Iranian nuclear reactor at Natanz which impact to slow

down the centrifuges by 1.000 centrifuges and bring them out of control(The Washington Post, 2012). The discovered system which has been infected by this malware exceeds 16.000(The Washington Times, 2012). Furthermore, the Stuxnet affected more than 14 industrial firms in Iran such as a uranium-enrichment plant (Kushner, 2013).

Shamoon (Saudi Arabia)

Saudi Aramco considered as the one of the largest oil companies in the world according to some financial journals(OilVoice, 2011). The national security of the Kingdom of Saudi Arabia will be impacted if this company received threats as it is measured as a major Saudi Arabia CNI Company owned by the government. Shamoon malware targeted Aramco on August 15, 2012 as a cyber-attack attempt which results to wipeout 30.000 computers which caused Aramco employee to stop functioning and network services to be an unavailable for weeks which considered as national security threats to the Saudi government impacting the economic and cybersecurity reputation.(Dehlawi & Abokhodair, 2013)

Flame (Middle East)

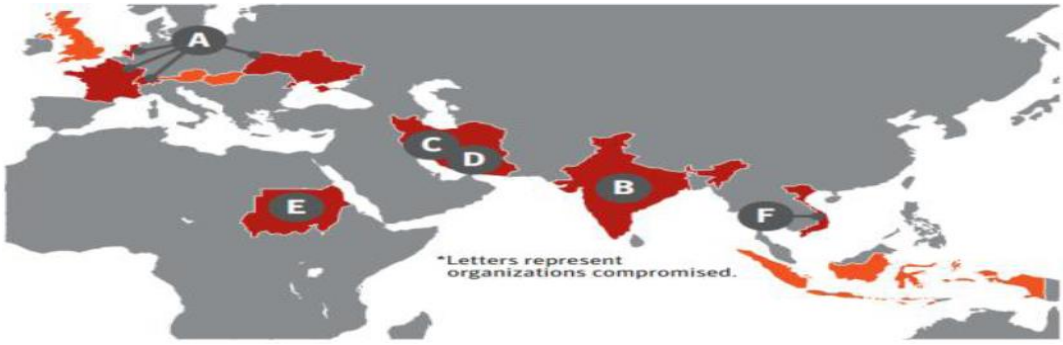
The Flame malware targeted the Middle East in 2012 and had been discovered by the national CERT of Iran which state that, this malware is targeting Critical National Infrastructures and can be used as a weapon to attack it(Maher, 2012). The Security & Defense Agenda published an article which states that the Kaspersky lab estimated 1000 to 5000 systems had been infected with Flame malware worldwide(SDA, 2012). Furthermore, the Flame malware targeted several of the vulnerabilities which were exploited by Stuxnet malware(First Stuxnet – Now the Flame Virus 2012). This malware impacted some critical industrials field like the oil sector and penetrated it aiming to achieve the following malicious activities:

1. Steal and attack various database
2. Audio Spying on the infected system
3. Capture the infected system screen and forward it to the attacker.
4. Do a keyboard monitoring activities
5. Monitoring Network traffic

Duqu (the Middle East and Europe)

Symantec states that in 2011 the Duqu Trojan has infected six organization within eight countries as shown
in the below graph(Symantec, 2011).

Figure7: The Graphical View of the Infected Organization with Duqu Trojan



Source: (Symantec, 2011)

The above graph represents the infected country and the organization by the Duqu Trojan. This Trojan considered as a Remote Access Trojan (RAT). It aimed to collect intelligence stored data and sensitive information from the targeted industrial infrastructure and its systems and open a backdoor to initiate a further attacks targeting the other connected organization within infected organization and used it as a distribution entry for the malicious code (Virvilis et al,2014).

Current approach

Local CERT

The Local Computer Emergency Radiance Team (CERT) within the countries aiming to enhance countries cybersecurity through analyzing cyber risk and security threats which may impact public, private or individuals(CERT Oman Natioanl, 2010). CERTs build the collaboration capability between other countries in responding to any cyber incident and sharing the relating finding in regards to cyber threats and vulnerabilities(CERT-UK 2013). The CERT organization within the countries supports the CNI organization by providing cyber security advice when they request it(CERT-UK, 2013).

Strength

The main strength of CERT is the availability of specialized and well-equipped teams that are available to respond to any cyber threats. Also, there are considering as a focal point for the local CNI to seek consultancy in any related matters of cybersecurity.

Limitation

The main concern in regards to the limitation of CERT is the covering of wide variety of cybersecurity incidents that may occur at the same time and since CERT support nation wise at a national level it will be a lot of areas to cover in a very limited time frame. Also, the limited number of specialist and team members is a critical factor to the quality of response to specific CNI threats. Furthermore, CNI networks are private and self-contained. Meaning CERT has no direct or live monitoring on their

networks, therefore, CERT will depend on the reported incident by the CNI organization and that will only happen after the threats have a successful infiltrated network.

Security Division (Local)

The security within the Critical National infrastructure organization is not the main concern of the management within that organization because they are focusing more on the production of the facility rather than the operations of the systems and its safety by the mean of the monitoring and handling the security concerns. Although, some organizations may have such department to which take care of information security aiming to mitigate the issues. However, the criticality remains by the shortage of specialist and expertise manpower whom they work in the security field.

Strength

The main strength within this approach is the familiarity of the team who is working in this department with the organization requirement, cultures, and structures. These advantages lead to respond and solve the faced security challenges very fast. Furthermore, Security Division within the organization it can play a major role on enhancing and applying the security best practice to meet the standards and align the Information security strategy with the business strategies without compromising the security level.

Limitation

The Security Division (Local) is focusing on daily operation and conducting routine works which make the team pussy with it. As a result, the security team will be outdated and not familiar with the new cyber challenges and the new methodology and techniques of attack that may target the organization. In addition to that, the collaboration and trust with other security team are missing. In some cases, the collaboration with other organization in related to security is needed to response to cybersecurity incident in a time manner, and this approach will not work alone without having a national center which considers the trusted center which provides the collaboration between the related parties.

Conclusion

In conclusion of this paper, the illustrations of the criticality of the topic can be understood now as there is much-shaded light to this topic by the end of this paper. Furthermore, the researcher only can conclude by pointing out a few of the most important points that might be an inspiration for coming researchers to pursue advanced research within this field. This research truly illustrated the importance of such studies on this filed that shows the criticality and the need for advanced methodologies and frameworks is highly on demand.

The critical national infrastructure also may have been referred to it as CNI. Currently the critical infrastructures; government and private depending on the internet and online connectivity to communicate with each other to share and exchange various collaborative services. However, with such connectivity, a number of threats have surfaced, that have become outstanding challenges for IT security and network admins who monitor these CNI Networks. The threats can be summed at

(various hacking attempts, a spread of malicious Scripts & malware, deliberate or malicious attacks on computers or network infrastructure.

Involuntary defects of computer systems or network infrastructure, due to personnel actions (human Error) or typical equipment failure. In any case, the end result may become fatal, and company level, but also could case tremendous consciences that may affect at national/international Level. As it has been illustrated the result may Couse economical distractions, political effects, etc.

Previously it has shown that the developed solution functioning as cyber detecting and monitoring tool that detected and viewed some of the real-time cyber-attack that targeted the monitored CNI infrastructures and services. The evaluation has been based on various methods of attacks along with the use of some common existing tools that simulate a security assessment of legitimate activities or hacking attempt as a malicious activity that could be conducted by any unauthorized personal/user. The main objective of this project is the attempted to formulate a complete solution which can be used to enhance the Cybersecurity within the CNI organization which can be considered as a strategy or framework that can be placed in the particle.

We acknowledge that existing framework requires further development both in academic circles and communities. After critical analysis of several countries CNI and extensive case studies it is clear that Oman's CERT monitoring system is better than other Middle East countries but not sufficient to protect from strong cyber-attack yet. Future studies can be possible by using different methodology and approaches. We consider that a tremendous opportunity for the research community to tackle the many open questions about Cyber security which we have laid out.

Corresponding Author
Name: Mohammad Imtiaz Hossain
Address: Faculty of Economics and Management, UPM. 43400, Serdang, Selangor, Malaysia.
Personal Email: imtiazhossain677@gmail.com
Institutional Email: gs53627@student.upm.edu.my

References

Bilge, L., & Dumitraş, T. (2012). Before we knew it: an empirical study of zero-day attacks in the real world. *Proceedings of the 2012 ACM conference on Computer and communications security* (833-844). ACM.

CERT-UK (2013). Coordination and Collaboration.Retrieved from: <https://www.cert.gov.uk/what-we-do/>.CERT-UK (2013).*CERT-UK.*Retrieved from <https://www.cert.gov.uk/>.

CERT, ON (2010), *Oman Natioanl CERT* .Retrieved from <http://www.cert.gov.om/about.aspx#.U41gmWbknmQ>.

CERT US (2014). *US Department of Homeland Security*. Retrieved from <http://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_%20Jan-April2014.pdf>.

Cornish, P., Livingstone, D., Clemente, D., & Yorke, C. (2011). Cyber security and the UK's critical national infrastructure.

Choo, K-KR (2010). 'High tech criminal threats to the national information infrastructure', *ELSEVIER*, vol. 15.Computer Fraud & Security (2001). *Elsevier Science Ltd*.

De Bruijne, M., & Van Eeten, M. (2007). Systems that should have failed: critical infrastructure protection in an institutionally fragmented environment. *Journal of contingencies and crisis management*, *15*(1), 18-29.
Dehlawi, Z., & Abokhodair, N. (2013). Saudi Arabia's response to cyber conflict: A case study of the Shamoon malware incident. In *2013 IEEE International Conference on Intelligence and Security Informatics* (pp. 73-75). IEEE.
Defense, USDo (2010). 'Quadrennial Defense Review Report', *Washington DC: Government Printing Office*, February.
Duroy, Q (2011), 'The Place of Biotechnology in Modern Civilization: A Veblenian Analysis of Public Misgiving Toward Embryology in the United States', *Journal of Economic Issues*, vol. 25, no. 3.
Ellen Nakashima, GMaJT (2012). *The Washington Post*.<http://www.washingtonpost.com/world/national-security/us-israel-developed-computer-virus-to-slow-iranian-nuclear-efforts-officials-say/2012/06/19/gJQA6xBPoV_story.html>.
Foster Jr, J. S., Gjelde, E., Graham, W. R., Hermann, R. J., Kluepfel, H. M., Lawson, R. L., ... & Woodard, J. B. (2008). *Report of the commission to assess the threat to the united states from electromagnetic pulse (emp) attack: Critical national infrastructures*. electromagnetic pulse (emp) commission mclean va.
GAO (2007).'Cybercrime: Public and Private Entities Face Challenges is Addressing Cyber Threats', *GAO-07-705*, June 27, pp. 5 - 12.
Hill, G (2013), 'Eavesdropping on enterprise apps', *sc magazine*, October 15, pp. 1-2.
Kimberly K. Peretti , DePalo, M. (2013). Evolving DDoS Attacks Provide the Driver for Financial Institutions to Enhance Response Capabilitie , *The Banking Law Journals*, 513-515. A.S. Pratt & Sons Publication
Kushner, D (2013). 'The Real Story of Stuxnet', *IEEE*, p. 53.
Liang, G., Weller, S. R., Zhao, J., Luo, F., & Dong, Z. Y. (2017). The 2015 ukraine blackout: Implications for false data injection attacks. *IEEE Transactions on Power Systems*, *32*(4), 3317-3318.
Labs, N (2013). *NSS LABS*, <https://www.nsslabs.com/>.
Maher(2012).Retrievedfrom <http://www.certcc.ir/index.php?name=news&file=article&sid=1959>.
Map(2013).*Digital Attack Map*, December 26, <http://www.digitalattackmap.com/#anim=1&color=0&country=ALL&time=16065&view=map>.
OilVoice (2011). *The Top 5 Oil Super Majors*, August 20, <http://www.oilvoice.com/n/The_Top_5_Oil_Super_Majors/384aab92e.aspx#gsc.tab=0>.
Rinaldi, S. M., Peerenboom, J. P., & Kelly, T. K. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE control systems magazine*, *21*(6), 11-25.
Singh, A. N., Gupta, M. P., & Ojha, A. (2014). Identifying critical infrastructure sectors and their dependencies: An Indian scenario. *International Journal of Critical Infrastructure Protection*, *7*(2), 71-85.
Shakarian, P., Shakarian, J., & Ruef, A. (2013). *Introduction to cyber-warfare: A multidisciplinary approach*. Newnes.
Stevens, T. (2013). Cyberspace and national security: threats, opportunities, and power in a virtual world SDA(2012).*Security Defence Agenda*, 05 29,

<http://www.securitydefenceagenda.org/Contentnavigation/Library/Libraryoverview/tabid/1299/articleType/ArticleView/articleId/3146/Most-sophisticated-cyberattack-yet-discovered.aspx>.
Security (2011).'Cyber Security Strategy for Germany', *Federal Office for Information Security*.
Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences*, *80*(5), 973-993.
Symantec (2011). *Duqu: Status Updates Including Installer with Zero-Day Exploit Found*, Nov 01, <http://www.symantec.com/connect/w32-duqu_status-updates_installer-zero-day-exploit>.
The Gulf News (2017).Oman thwarted over 880m cyber attacks in 2017. Retrieved from: https://gulfnews.com/world/gulf/oman/oman-thwarted-over-880m-cyber-attacks-in-2017-1.2254863
The washington times (2012). <http://www.washingtontimes.com/news/2012/feb/18/iran-says-stuxnet-virus-infected-16000-computers/>.
The Washington Post (2012. <http://www.washingtonpost.com/world/national-security/us-israel-developed-computer-virus-to-slow-iranian-nuclear-efforts-officials-say/2012/06/19/gJQA6xBPoV_story.html>.
U.S. State and Federal Government Cybersecurity Report (2017).
SecurityScorecard
https://cdn2.hubspot.net/hubfs/533449/Images/SecurityScorecard%202017%20Govt%20Cybersecurity%20Report.pdf
Yunos, Z., Ahmad, R., Suid, S. H., & Ismail, Z. (2010). Safeguarding malaysia's critical national information infrastructure (cnii) against cyber terrorism: Towards development of a policy framework. In *2010 Sixth International Conference on Information Assurance and Security* ,21-27, IEEE
Virvilis, N., Vanautgaerden, B., & Serrano, O. S. (2014). Changing the game: The art of deceiving sophisticated attackers. In *2014 6th International Conference On Cyber Conflict (CyCon 2014)* ,87-97, IEEE.
Wueest, C. (2014). Targeted attacks against the energy sector. *Symantec Security Response, Mountain View, CA*.