ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 12, December 2019

An Assessment of Cyber Attacks Preparedness Strategy for Public and Private Sectors in Zambia

Kingstone Ali Mwila[1], Charles S. Lubobya[2]

P.G. Student, Department of Electrical and Electronics Engineering, School of Engineering, University of Zambia, Lusaka, Zambia[1]

Head of Department, Department of Electrical and Electronics Engineering, School of Engineering, University of Zambia, Lusaka Zambia[2]

ABSTRACT: The growing dependence on the cyberspace makes preparedness strategy against cyber-attacks important to achieve security objectives. The cyberspace has become one of the targets for cyber-attacks. Critical Infrastructure services such as banks, power grid, utility, telecoms, and many others. The strategies for preparedness again cyber-attacks in involve legal and regulatory framework, compliance to standards, technical, organizational, capacity building, and cooperation aspects. The nature and form of cyber-attacks are becoming advanced persistent threats. The strategy against cyber-attacks demands long-term coordinated efforts from the decision-makers, including vision, strategy, and investment prioritization as well as the organizational agility to respond to ever-changing tactics and techniques. The cyber preparedness strategy enables an organization to identify the nature and the forms of cyber-attacks; develop preparedness strategies against cyber-attacks setting objectives; and develop a model that can be used to curb cyber-attacks. This paper is An Assessment of Cyber Attacks Preparedness Strategy for Public and Private Organisations in Zambia.

KEYWORDS: Cybersecurity, Critical infrastructures, Weapons, cyber-attacks.

I. INTRODUCTION

Cyber-attacks are one of the most devastating threats to the nations. Its impact affects critical infrastructures and services [1]. The most common critical information infrastructures are power plants, telecommunications systems, health systems, banking and financial systems, and others which are connected for data sharing [1].
Cyber-attacks preparedness involves the capabilities of proactive and reactive operations to achieve confidentiality, integrity and availability of the computing resources. It helps to identify the weapons used to attack the targets [27]. The weapons range from denial of service, malware, ransomware, worms, and others [3]. It also provides the development of processes, methodology, standards, techniques, and mechanism that forms a sense of alertness, to plan, to identify, and defend critical cyberspace infrastructures and services. The study establishes the immediate approach to explore and outline forms of cyber-attacks capabilities that would possibly threaten networks in the public and private sectors in Zambia and what potential effects they may have. The cyberspace requires coordinated efforts to manage because it is borderless in its nature. Therefore, there is need to apply standards and best practices to achieve security objectives.

The purpose of the study is to assess cyber-attacks preparedness strategies in the public and private sectors in Zambia as the country continues to expand its service delivery and using critical infrastructure and services. The intention is to identify whether Zambia utilizes cyber-attacks readiness resources in an optimal manner. The general objective of the study is to assess cyber-attacks preparedness for the public and private organisations in Zambia.
This study will be guided by the following objectives; to identify the nature and the forms of cyber-attacks; to evaluate the existing preparedness strategies against cyber-attacks; and to develop model that can be used to curb cyber-attacks.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 12, December 2019

II. RELATED WORK

The Internet has become a target for strategic attacks among countries that are figuring prominently in the security and safety strategies, and companies are investing billions [4]. Data storage, transfer, and processing are really driven by the increased dependence on the Internet, from controlling our armed forces to trade, e-commerce, social communication. Everything relies on the Internet. We are in some ways dependent on the Internet today [5], [28]. Attackers exploit the Internet to achieve their agenda. The most-reported cyber-attacks the motives behinds are different some are regarded a political, activism, sabotage, state-sponsored, and more [29]. Cyber warfare-attacks are not only associated and initiated by military operations, but the civilians who know what they are doing are also launching cyber warfare-attacks. With the increase of easy to use the tool on the internet, anyone with an attacking motive can launch a cyber-attack [6].

Cyber-attacks

The cyber-attacks that have occurred in the past years have shown the vulnerabilities of using the internet and the weaknesses of cyber defenses [4]. Cyber-attack is an action taken to harm a computer network for a political, sabotage, protect against something, for financial gain and others [30]. It is also a security breach in the cyberspace. Computer network vulnerabilities, if are found, are usually exploited to undermine the function of the system. Some of the vulnerabilities used are known as 'zero-day' as they had not been uncovered or made known to the developers. Stuxnet, for example, was found to use a total of four zero-day vulnerabilities [7].

Cyber-attack preparedness

The United States (U.S) Commerce Department of the National Institute of Standards and Technology (NIST) has a Framework used for Infrastructure Cybersecurity, called the Cybersecurity Framework [37]. The Cybersecurity Framework cab be prioritized, flexible, and economical to support the protection and resilience of its essential infrastructure and totally [8]. See Figure 1

Figure 1: NIST Cybersecurity Framework Version 1

The Framework Core is structured into five Functions that identify the key cybersecurity outcomes identified to manage cybersecurity risk [37, 38], [9]:

- **Identify** – develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.
- **Protect** – develop and implement the appropriate safeguards to ensure the delivery of critical infrastructure services.
- **Detect** – develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 12, December 2019

- **Respond** – develop and implement the appropriate activities to take action regarding a detected cybersecurity event.
- **Recover** – develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

The United Nations Agenda to Cybersecurity

The International Telecommunications Union (ITU), Global Cybersecurity Agenda (GCA) has released a framework or model which is generic for international multi-stakeholder and its member state on cybersecurity [34], [39]. The aim is to build synergies with current and future initiatives and members with the sense of security assurance in the cyberspace and information society. Below are Work Areas of the GCA:

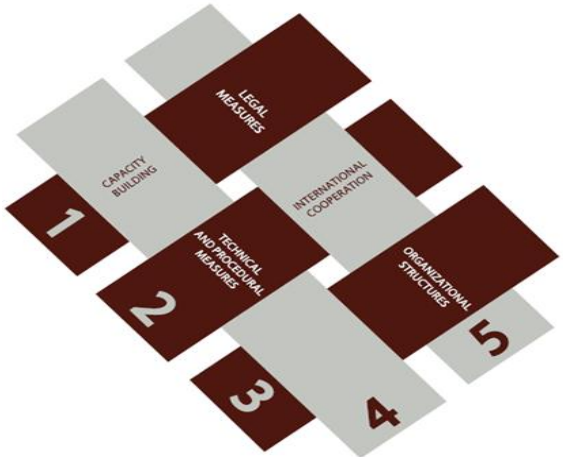


Figure 2: ITU CGA Model

- **Legal Measures**: This Pillar seeks to elaborate methods for the event of model globally applicable and practical crime legislation.
- **Technical and Procedural Measures**: This Pillar focuses on measures for addressing vulnerabilities in software system merchandise acceptable enfranchisement schemes, protocols and standards.
- **Organizational Structures**: The Pillar aims to form organisational structures and techniques to assist forestall, discover and reply to attacks against essential info infrastructures.
- **Capacity Building**: This Pillar seeks to elaborate methods for enhancing information and experience to spice up cybersecurity on the national policy agenda.
- **International Cooperation**: The Pillar focuses on methods for international cooperation, dialogue and coordination.

Why Cyber-attacks are On the Rise

The continuous advancement in technology has shifted the way humans live and behave. Most human activities depend on the usage of technology [31], [32]. The world is connected like never before. Everything is connected. Humans are connected to humans, humans are connected to machines, machines are connected to humans, and machines are connected to machines [9]. The ignorance of the users which is taken by lack of awareness is another form that causes attackers to gain easily into the targeted systems and cause harm or fulfil the intentions [10].

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 12, December 2019

Sources of Cyber Warfare Weapons

Actors who consciously decide to conduct cyber-attacks can potentially cause harm for any system which directly or indirectly is connected to the Internet [34, 39]. See Figure 3. The diagram below shows source of cyber-attacks.

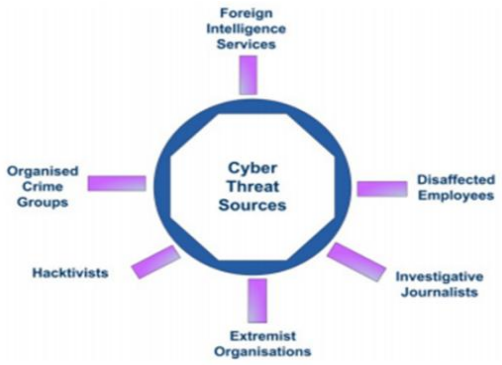


Figure 3: Source of cyber-attacks (Credit ITU) [34]

Forms and Nature of Cyber Attacks

The Forms and Nature of Cyber Attacks are Offensive in nature to destroy, disrupt or neutralise the target as close to their source as possible [11]. Attackers always have an advantage when successfully exploited the vulnerabilities, gains access and clear the marks. They only need to find one hole to penetrate a system, while those who defend the system must locate and seal all holes [12]. The techniques for cyber offensive operations, including network intrusions, malware, botnets, and denial-of-service (DoS) attacks [13]. The method of attack is determined by the objectives and the type of vulnerabilities exploited [14], [15]. An attacker can spend weeks, months or even years to study the targeted network and come up with the method that can help to break into the system. They can also be formed as offensive weapons [16]. These include the espionage, propaganda, denial-of-service (DoS), data modification and infrastructure manipulation [17].

Motives for Cyber Attacks

The actors of cyber-attacks also refer to as 'hackers' (whether for financial gain or as a challenge), cause-based groups, proxies for governments, and governments (including their military and intelligence agencies) [34]. The motives for the attacks range from financial gain to the advancement of national security interests, to the satisfaction of peer recognition, and to the advancement of various causes [18], [36]. To understand to motives it is important to ask a question: Is a Cyber War taking place right now or about to begin? Who is attacking? What is the target? What kind of attack methods is being used? [19].

Historic Case Reviews

The growth of the internet of things in the twenty-first century is a growing cyber-attacks nightmare [20]. The historical events have proved that cyber-attacks exist with the involvement of military and non-military weaponisation: Chechnya Propaganda of 1994; Military Hacking In Kosovo War of 1999; Cyber Warfare in the Middle East in 2000; Tension between US and China in 2001; Iranian Stuxnet worn attack in 2005; Estonia Hacking On Government and Private Institutions in 2007; First Cyber- attack in Georgia 2008; Ukraine Christmas Power Outage in 2015; Liberian Cell Phone Network Operator Was Shut Down in 2015.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 12, December 2019

Standards and Best Practices

It is important to identify, establish and implement the useful best-practices, standards and guidance for effective cybersecurity. Those should be able interacting with other standards and guidance [21], [25]. Most of the standards are can be customised to any organization regardless of the size or the industry and sector in which they operate [22].

The National Institute of Standards and Framework's Cybersecurity Framework (CSF) NIST CSF. The ISO/IEC 27000 family of information security standards of information security management standards) is a series of mutually supporting information security standards that can be combined to provide a globally recognised framework for best-practice information security management [34,35]. ISO/IEC 27001 - the international Standard for best-practice information security management systems (ISMSs). ISO/IEC 27032 - standard focuses explicitly on cybersecurity but does not as precise or prescriptive recommend as those supplied in ISO/IEC 27001. ISO/IEC 27035 - the standard for incident management and forms the crucial stage of cyber resilience. ISO/IEC 27031 - the Standard for organizational preparedness for business continuity and a logical step to proceed from incident management, as an uncontrolled incident can transform into a threat to ICT continuity. ISO/IEC 22301 - the Standard for business continuity management systems (BCMSs), and forms the final part of cyber resilience. This Standard not only focuses on the recovery from disasters, but also on maintaining access to, and security of, information, which is crucial when attempting to return to full and secure functionality.

African Union Convention on Cyber Security and Personal Data Protection

National Cybersecurity Frame Work

National Policy: Each state shall undertake to develop, in collaboration with stakeholders, a national cybersecurity policy which recognises the importance of Critical Information Infrastructure (CII) for the nation identifies the risks facing the nation using the all hazard approach and outlines how the objectives of such policy are to be achieved [33, 39].

National Strategy: State parties shall adopt the strategies they deem appreciate and adequate to implement the national cyber security policy, particularly in the area of legislative reform and development, sensitization and capacity building, public-private partnership, and international cooperation, among other things. Such strategies shall define organizational structures, set objectives and timeframes for successful implementation of the cybersecurity policy and lay the foundation for active management of cyber security incidents and international cooperation [23], [26].

SADC Cybersecurity

The Southern African Development Community (SADC) Secretariat to continue promoting capacity building initiatives relating to cyber security; The SADC Secretariat urged to develop a list of harmonized indicators to measure progress in cyber security commitment of all SADC Member States and to include these indicators under the SADC ICT Observatory; The SADC Secretariat urged to develop a SADC Model Cyber Security Strategy that would be utilized by SADC Member States in developing their own National Cyber Security Strategy [24].

III. METHODLOGY

The data collection in this study was achieved by the using of quantitative and qualitative methods which employed survey questionnaires both physical and face to face interviews of selected companies in Zambia's public and private sectors. The interview questions were purposefully designed to give the organizational level status in the adoption and or implementation of cybersecurity best practices and standards. This gave assessment so as to be able to recommend the right controls for the mitigation against cyber-attacks.

The targeted population in the organizations where the Chief Information Security officers, information security professionals, Cybersecurity professionals, Network Administrators, IT Auditors, Computer Engineers, End Users and other related professionals who are directly involved in administration and management cybersecurity, Top management, Finance, Legal and Training.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 12, December 2019

Questionnaires were generated in line with the required research information. These included questions for assessing the extent to which internal Cyber security assurance enhances, assessing the influence of Cyber security recommendations on corporate strategy against cyber-attacks in the organization.
The statistical values of the obtained results were analyzed, processed and verified using Microsoft Excel. Thereafter, the cyber-attacks preparedness model was proposed with the concentration on strategy, using the designed assessment activity from the previous chapters.

IV. RESULTS AND DISCUSSIONS

The study focused on a sample population response from the Health - 2%; Consumer Products and Services - 16%; Manufacturing, Mining, Construction and Engineering - 4%; Government (Regulator, Law enforcement, Defense) - 23%; Energy (Oil, gas, power, utility) - 4%; Telecommunications (ICT, ISP, Software, Telecoms) - 34% industries as well as those in the banking and financial sector - 2%.

The findings of this study was organized according to the objectives: to identify the nature and the forms of cyber-attacks; to evaluate the existing strategies used in preventing cyber-attacks; and to develop a model that can be used to curb cyber-attacks. Among the respondents interviewed were IT specialists, IT Auditor, Cybersecurity Professionals, Chief Information Security Officers, and among computer users

Nature & Forms of Cyber-attacks
Majority of the respondents in excess of 77.2% had indicated that their managers had placed high priority on cyber security. Only 50% of respondents that indicated that their Organization had sought information, advice or guidance on the cyber security threats in their Organization in the previous 12 months. The rest either had not sought for such information or were not so sure whether their Organizations had sought for such information or not.
Findings of the study revealed a number of cyber-attacks forms had been experienced in a number of institutions with the most common forms of warfare attacks being fraudulent emails or data being directed to fraudulent websites, with 55.3% of the respondents indicating that they had experienced it. Further, 48.2% of the respondents indicated that they had experienced attacks in form of Spyware, Malware or Ransomware.

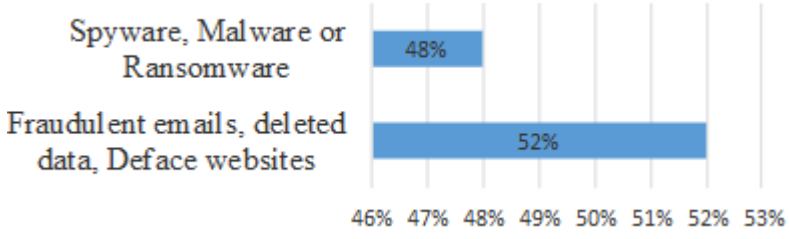


Figure 4: Nature and forms of cyber attacks

Other common forms of cyber-attacks reported or experienced in the organizations from which the study was conducted include: Hacking of online bank accounts, denial-of-service attacks, impersonating organization in emails, viruses, unauthorised use of computer networks or servers by outsiders, unauthorised manipulation of customer records, and other breaches.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 12, December 2019

Frequency of Attacks

How often in the last 12 months, did you experience cyber security breaches or attacks?

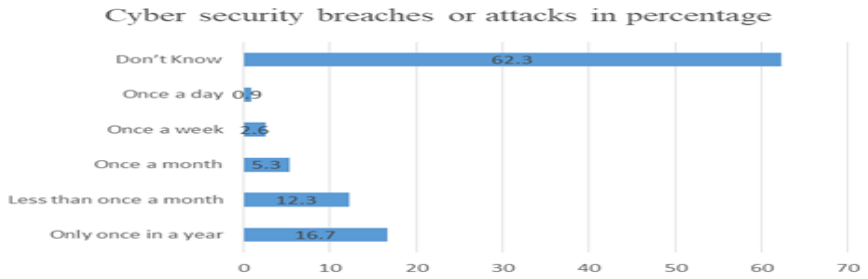


Figure 5: Cybersecurity breaches. The number of frequency and experience of cyber-attacks in the last 12 months.

Effects of the Cyber Attacks

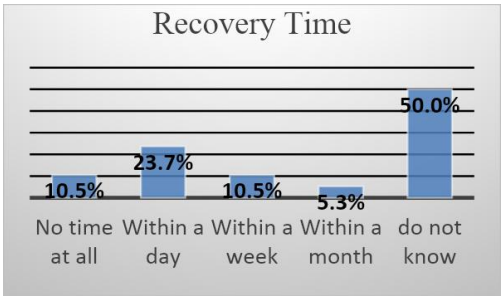
The study established that such security breaches and attacks had resulted in the following: Fraudulent emails and data being directed to fraudulent websites; Loss of revenue or money; Lost or stolen assets, trade secrets as well as intellectual property. Temporary loss of access to files or networks. Permanent loss of files (not personal data). Software or systems corrupted or damaged, Website or online services taken down or slowed.

Further, in terms of the Organization itself, the following were the impact of such cyber-attacks: Staff members stopped carrying out daily work, thus preventing the efficient and effective provision of goods and services. Complaints from customers increased in number. This required that the Organization to do goodwill compensation to its customers. There were fines and legal costs that the institutions had to make. There was loss of revenue and share value. Lost man hours during the time of clearing the breaches and attacks.

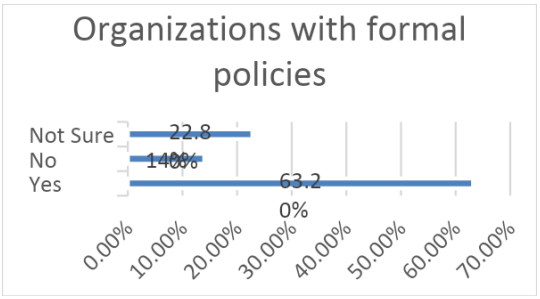
The Organization needed to come up with new measures in order to deal with any possible future attacks. There was communication breakdown both within and without the Institutions due to these cyber-attacks. The effects on the operations of the Organization further resulted in reputational damage of institutions.

Recovery Period

Regarding the most disruptive breach, or cyber-attack, it took different periods for different Organizations to address the problem and restore their normal operations upon identifying the breach. Refer to figure 6 a.



(a)



(b)

Figure 6 (a) Time taken to restore business to normal operations upon identifying the breach. (b) Organizations with formal policies or document for cyber security risks in any way.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 12, December 2019

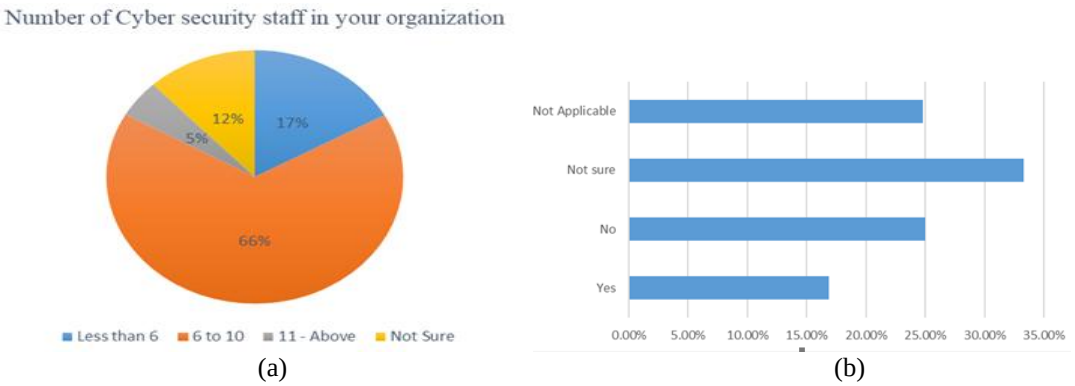
Existing Strategies in Preventing Cyber attacks
In order to establish appropriate model meant to curb cyber warfare it was also important to outline and analyse the existing strategies that Organizations are currently using. One such strategy that was analysed was the existence of formal policies or documents for cyber security risks.

Availability of Formal Policies Dealing With Cyber Security.
From the findings of the study, 63.2% of the respondents revealed that their organizations had formal polices and documents dealing with cyber security risks. 14% of the respondents stated that they had no formal policies or documents dealing with such, while 22.8% were not sure whether such policy documents were available in their Organizations or not. Figure 6 (b) above for detailed illustration of institutions with cyber security policy documents.

Issues Covered In the Cyber Security Policies
In terms of those with policies on cyber security risks, the following are the major available policies that are being used in these institutions: Devices Remote or mobile working; Document management systems; Use of new digital technologies such as cloud computing data classification; Restrictions in the use of personally owned devices such as USB sticks; Restrictions on what staff are permitted to do on the IT system of their organization; What can be stored on removable devices (example USB sticks).

Rules and Controls.
The study revealed that in order to identify cyber security risks, the following activities have been undertaken within these Organizations: Ad-hoc health checks or reviews beyond regular processes; Internal and external audit; Business-as-usual health checks that are undertaken; Risk assessment covering cyber security risks; Invested in threat intelligence to your organization; SMS blasts to customers warning them against fraudsters.
Further, the following rules and control systems were put in place in order to enhance the security systems against cyber-attacks. Access/Role based rules where access was only allowed via company owned devices. Applying software updates when they are available. Up-to-date malware protection; Ensure the Firewalls available are with appropriate configuration; Restricting IT admin and access rights to specific users; Backing up data securely via other means; Guidance on acceptably strong passwords; Security controls on company owned devices (example laptops).

Establishment of Cyber Security Departments in the Institutions.
Regarding established cyber security departments within the Organizations under study, findings revealed that 72.8% of the respondents indicated that they had cyber security departments in their Organizations, while only 20.2% indicated that they did not have such departments in their Organizations. Only 8% of the respondents were not sure about the existence of such departments in their Organizations.



(a) (b)

Figure 7: (a) Do you have an Information/Cyber Security Department in your Organization? (b) Number of Cyber security staff in your organization

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 12, December 2019

Training on Cyber Security

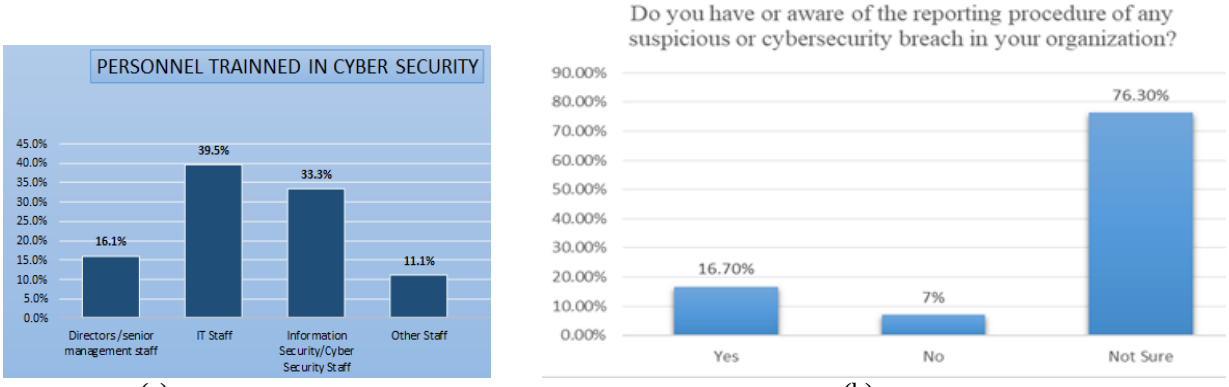
(a) (b) (c)

Figure 8: (a) Whether people dealing with cyber security have the right skills and knowledge to do this job effectively. (b)Training and skills on cyber security. (c) Organizations where staff have had cyber security training in the last 12 months?

Personnel Trained in Cyber Security

Of those that had had cyber security training, the study revealed that the highest number of staff trained in Cyber security were those from Information Technology Departments (IT staff) in excess of 39.5%, while the least number of cyber security trained staff were from other staff with 11.1%. Results further revealed that 16.1% of the Directors, and 33.3% of Cyber/information security staff in the institutions under study had received training in cyber security. See figure 4 below for detailed illustration of the findings.

Ideally, it would be expected that the highest number of people trained in cyber security are those in the cyber security department. However, contrary to this expectation, results reveal that this department has a lower number of people that received training in cyber security in as far as the institutions under study are concerned. Given that, results revealed that the majority of respondents in excess of 72.8% indicated that they have cyber security departments; this abnormally could be an indication that most Organizations have misplaced their training priorities in other departments that are not cardinal in ensuring cyber security in these institutions, while ignoring the critical department such as the Cyber Security department itself.



(a) (b)

Figure 9: (a) Personnel trained in Cyber Security (b) Do you have or aware of the reporting procedure of any suspicious or cybersecurity breach in your organization?

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

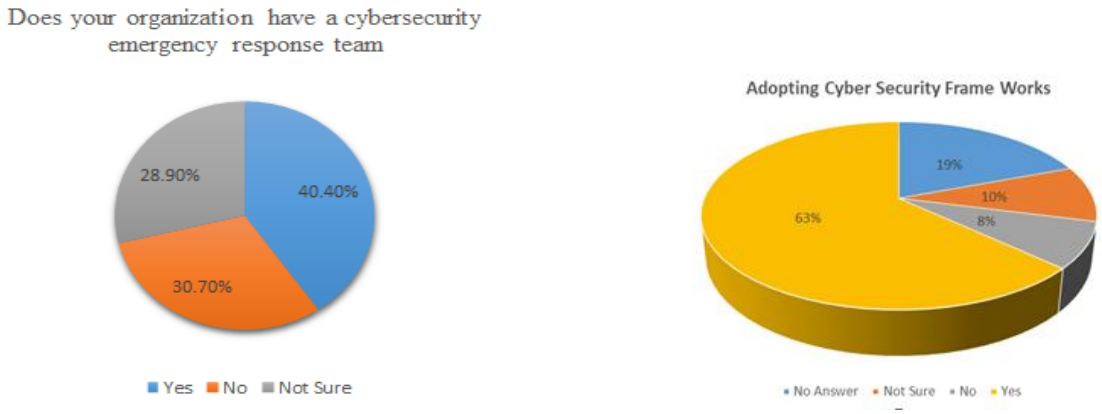
(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 12, December 2019

Reporting and Responses to Cyber Security Attacks

However, even though most of these Organizations lacked the reporting procedures largely, results revealed that 40.4% of the Organizations under study have a cyber-security emergency response team, which is responsible for any unforeseen emergency cyber-attacks within the Organizations. Further, that 30.7% did not have this cyber security emergency response team, while 28.9% were not sure whether such a team was available in their Organization. See table figure 9 b above and figure10 a below for detailed illustration.



(a) (b)

Figure 10: (a) Does your organization have a cybersecurity emergency response team. (b) Do your organisation have a framework or standards, if any, do you require you organisation and supplier to have or adhere to?

Adoption of Cybersecurity Frameworks, Standards and Best Practices

In terms of those with cybersecurity frameworks, standards and best practices, the following are some of the major available cybersecurity frame works, standards which institutions adopted within and that of their suppliers: Payment Card Industry Data; Security Standard (PCI DSS); Recognised standards such as ISO 27000 series; National Institute of Science and Technology Cyber Security Frame Work; Independent service auditor's report such as ISAE 3402; COBIT Framework; ITIL Frame Work

The findings revealed that 63% of the respondents indicated that they had cyber security framework in their Organizations, while only 19% did not indicate whether such frame works are used in their Organizations. Only 10 % of the respondents were not sure about the existence of such frame works in their Organizations. Further, 8% did not have any cyber security frameworks or best practices. See figure 10 b above

The results about the adoption and implementation of cyber security frame works, standard and best practices in these organizations showed consistency, and reveals the fact that generally, Organizations were doing very little to ensure and to enforce effectively the cyber security frame works in their Organizations. The inefficient use of the frameworks is as a result the people handling cyber security are general IT specialists. It requires those with high level of understanding and competences, the cyber security specialists.

V. RECOMMENDATIONS

The research study set out the objectives and to answer the five research questions outlined in chapter one. The National Institute of Science and Technology (NIST) have developed a cybersecurity framework version 1.1 designed to detect, identify, intercept, and destroy or negate harmful activities attempting to penetrate or attack through cyberspace [39], [34]. This study, therefore, attempted to evaluate the extent to which organizations are keeping up to this challenge.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 12, December 2019

From the findings of the study, it was established high frequency into negative effects both on the operations as well as on the infrastructure and services of the Organization. These effects range from loss of data, financial loses, software systems damage, and websites slowed or brought down. This has further resulted in work derailment, as high operational costs as well as the loss of revenue and profits, among other things. Such findings resonate with observations made by various literature on the impact of cyber-attacks in affecting the critical infrastructures and services.

We recommend that decision-makers and the enterprises consider strategically to exhibit commitment and support in directing cybersecurity by providing frameworks, appropriate budget, and tools which are approved. The research identified Banking and Finance, Power and Energy, Health, Utility, Telecoms, government agencies are critical in restructures.

A complete comprehensive framework must be implemented from end to end. ICT security needs to be aligned to all developments and procedures organizational-wide. User awareness programs need to be the top of the security agenda for all business associates in a quest to be prepared and have a resilient environment.

The framework captures the Function Strategy, Capacity Building, Technology, Intelligence, Operational Protection, Operational Detection, Operational Response, and Recovery. The Proposed model can be used government agencies and private corporation in Security Operation Centre (SOC), which go by many names: Computer Security Incident Response Team (CSIRT), Computer Incident Response Team (CIRT), Computer Security Incident Response Capability (CSIRC), Network Operations and Security Center (NOSC), and, of course, Cyber Security Operation Centre (CSOC).

Proposed Cyber-attacks preparedness Model

We have depicted the model proposed from the International Telecommunications Union, Nation Institute of Standard Technology, combined with ISO 27000 Series, COBIT 5 Framework and many others. The mode shows that the key critical infrastructure and services either provided by the public or the private are protected. It expands its capabilities in line with two-way defense mechanisms (symmetric and asymmetric) in order to overcome internal and external threats.

Cybersecurity Strategic planning: Give the CSOC the authority to do its job through the effective organizational placement and appropriate policies and procedures.

Security Program Knowledge: Favour staff quality over quantity, employing professionals who are passionate about their jobs, provide a balance of soft and hard skills, and pursue opportunities for growth.

Cyber Security Technology and Operation Awareness: Consolidate functions of incident monitoring, detection, response, coordination, and computer network defense tool engineering, operation, and maintenance under one organization, Cyber Security Comand Centre. Realize the full potential of each technology through careful investment and a keen awareness of—and compensation for—each tool's limitations.

Identification and Intelligence Gathering: Exercise great care in the placement of sensors and collection of data, maximizing signal and minimizing noise. Be a sophisticated consumer and producer of cyber threat intelligence, by creating and trading in cyber threat reporting, incident tips and signatures with other CSOCs.

Cyber Security Operation and Protection: Carefully protect CSOC systems, infrastructure, and data while providing transparency and effective communication with constituents.

Operation Detection and Precautions: Achieve a balance between size and visibility/agility, so that the CSOC can execute its mission effectively. Carefully protect CSOC systems, infrastructure, and data while providing transparency and effective communication with constituents.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 12, December 2019

Operational Security Response: Respond to incidents in a calm, calculated, and professional manner.
Operational Recovery: It is a recovery of specific parts of the IT infrastructure in the case of an IT failure or a relatively a cyber-attack. The recovered data can have various forms: a file, an email message, a database entry, and other critical systems. See figure 11

Figure 11: Proposed cyber-attacks preparedness model (CAPM)

How to use the Model

The model is meant to offer the course of action to cybersecurity. The CAPM with an associated ITU, NIST, ISO 27000 series and other models can be used to describe cyber activity in a consistent and repeatable fashion. The framework can: Establish a shared ontology and enhance information-sharing. It is far easier to map the translation of multiple models to a common reference than directly to each other; Can support missions ranging from strategic decision-making to analysis and cybersecurity measures and users from generalist to technical experts. Support common situational awareness across organizations. Accommodate a wide variety of data sources, threat actors and activity; provide a foundation for analysis and decision-making; Provide a starting point for organizations that have not yet adopted a Security Framework. Built around the simple model and value-neutral concepts, against CAPM can be customized for an organization's needs and these modifications from the original against CAPM are readily apparent, facilitating mapping and data exchange.

Implementation of Effective Cyber Attacks Preparedness Model

- Welcome the cyber Attacks preparedness by the Executive officials in the business strategy.
- Align the model with other known standards and best practices.
- Alight the model in increase Return on Investments and increased asset security.

How the Model Was Developed

The idea of creating a **Cyber Attacks Preparedness Model**/framework came from observations among the National ICT Master Plan, National Seventh Development Plan that cybersecurity was not being described fully by different agencies in a variety of ways that made inconsistent understanding and addition suggestions of the model. There are over different standards and models being used across government, academia, and the private sector. Each model reflects the priorities and interests of its developer, but the wide disparities across models made it difficult to facilitate efficient situational to the industry. A typical operation includes the following elements:

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 12, December 2019

1. Prevention of cybersecurity incidents through proactive: a) Continuous threat analysis; b) Network and host scanning for vulnerabilities; c) Countermeasure deployment coordination; d) Security policy and architecture consulting.
2. Monitoring, detection, and analysis of potential intrusions in period and thru historical trending on security-relevant knowledge sources.
3. Response to confirmed incidents, by coordinating resources and directing the use of timely and appropriate countermeasures.
4. Providing situational awareness and reporting on cybersecurity status, incidents, and trends in adversary behaviour to appropriate organizations.
5. Engineering and operating CND technologies such as IDSes and data collection/ analysis systems [36].

The Relationship between CAPM and other Cyber Security Models

While NIST and other models have not promulgated or endorsed a specific **Cyber Attacks Preparedness Model**, it advocates the use of a cybersecurity framework in addition to a cybersecurity framework to inform risk decisions and evaluate safeguards and actions taken. NIST and other models offers the documentation that describes threat frameworks that offers depth understanding into that safeguards are additional necessary at a given purpose in time and specific threat circumstances.

CAPM and CSIRTs/CERTs

Garry Mukelabai [40] suggested that there is a need to recognize that improving Cybersecurity is a national and global problem and that each country in the region must improve its national efforts and undertake actions to hitch and support regional and international efforts to boost Cybersecurity. 1. Develop a national Cybersecurity strategy; 2. Review and, if necessary, revise current cyber legislation and draft new legislation, to criminalize the misuse of ICTs, taking into account the rapidly evolving Cybersecurity threats and; 3. Develop incident management capabilities with national responsibility and use current samples of (Computer Security Incident Response Team/Computer Emergency Response Team) CSIRTs/CERTs once developing these. There is a need to raise awareness about the existence of these national response teams.

Cyber Attacks Incident Management Capability

Computer Emergency Response Team with Sectors Specific CERTS report to National CERT to use the CAPM

Figure 12: Proposed Computer emergency response team [40] (Credit Garry Mukelabai)

Duties of a CERT

A central, trusted organisation that co-ordinates the response to Cybersecurity incidents. Also assists in proactive measures to reduce risk. Watch, Warning, Information Alert; Investigation & incident Response; Information Sharing and Analysis Centre

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 12, December 2019

VI. CONCLUSION

In conclusion, Cyber-attacks Preparedness Mode is an important tool for the protection of critical infrastructures and services of the state and business communities. The cyberspace with all the connected devices and services have continued to be platforms that require sound and proper protection mechanisms to provide security assurance. The evolution of cyberspace has continued to positively impact our society and has greatly changed the way we live, learn and conduct our everyday business. This applies to the private and public sectors. Critical infrastructures have been identified as a valuable resource that would foster economic and social development in a nation and connect the nation to other parts of the words. From the literature that has been reviewed, it has been established that critical infrastructures and services have become targets for cyber-attacks. It would furthermore benefit if these critical infrastructures and services are given primary attention by applying appropriate cybersecurity defense mechanism.
However, despite the importance of having smart cities, the Internet of Things and implementing ICTs being well known to policymakers, its security has been threatened by a lot of cyber-attacks that need the intervention. The country needs to deliberately come up with measures that can bring about and promote a well-established security assurance to critical infrastructures and services that would result in the secure national cyberspace. In this fourth industrial revolution era, the Internet is used as a medium for the transmission, storage, and sharing of resources. Some of these resources are highly valued for the governance of the state, businesses and the individuals. There are different groupings interested in such valuable sources including nations, companies, and individuals. The term cyber warfare may not only be applied to military spheres but civilians are waging this war just by applying their skills and knowing what they want.

REFERENCES

1. D. J. Bodeau, "Improving cyber security and mission assurance via cyber preparedness (cyber prep) levels," Proceedings - SocialCom 2010: 2nd IEEE International Conference on Social Computing, PASSAT 2010: 2nd IEEE International Conference on Privacy, Security, Risk and Trust, pp. 1147-1152, 2010.
2. S. Cheang, "Conceptual model for cybersecurity readiness assessement for public institutions in developing country: Cambodia," ICCIT 2009 - 4th International Conference on Computer Sciences and Convergence Information Technology, pp. 1411-1418, 2009.
3. R. Daley, "Operationalizing the coordinated incident handling model," 2011 IEEE International Conference on Technologies for Homeland Security, HST 2011, pp. 287-294, 2011.
4. M. Dion, "Intelligence and Cyber Threat Management," in Cybersecurity Best Practices, Springer Fachmedien Wiesbaden, 2018, pp. 363-392.
5. M. P. Efthymiopoulos, "A cyber-security framework for development, defense and innovation at NATO," Journal of Innovation and Entrepreneurship, vol. 8, no. 1, 2019.
6. G. Griffith, "Information technology preparations for the Pluto encounter from mission operations to science retrieval," in IEEE Aerospace Conference Proceedings, 2017.
7. C. E. Irvine, "Call in the cyber national guard!," IEEE Security and Privacy, vol. 8, no. 1, pp. 56-59, 2010.
8. J. Krüger, The secure information society: Ethical, legal and political challenges, vol. 9781447147, The Secure Information Society: Ethical, Legal and Political Challenges, 2013, pp. 1-213.
9. N. Kshetri, "The quest to cyber superiority: Cybersecurity regulations, frameworks, and strategies of major economies," The Quest to Cyber Superiority: Cybersecurity Regulations, Frameworks, and Strategies of Major Economies, no. September 2014, pp. 1-240, 2016.
10. G. M. Mancini, "Cyber and Chemical, Biological, Radiological, Nuclear, Explosives Challenges," pp. 311-325, 2017.
11. T. c. s. m. a. r. tool(CyberSMART), "Marshall, Jim," in Proceedings - Cybersecurity Applications and Technology Conference for Homeland Security, CATCH 2009, 2009.
12. J. A. Mattson, "Cyber defense exercise: A service provider model," in IFIP International Federation for Information Processing, 2007.
13. R. McDonald, "New considerations for security compliance, reliability and business continuity," in Papers Presented at the Annual Conference - Rural Electric Power Conference, 2008.
14. L. McLeod, "Reconceptualising security?," Gender Politics and Security Discourse, pp. 70-90, 2018.
15. N. Mehravari, "Resilience management through use of CERT-RMM & associated success stories," 2013 IEEE International Conference on Technologies for Homeland Security, HST 2013, pp. 119-125, 2013.
16. G. Mezzour, "Remote assessment of countries' cyber weapon capabilities," Social Network Analysis and Mining, vol. 8, no. 1, 1 December 2018.
17. J. Mouton, "The identification of information sources to aid with Critical Information Infrastructure Protection," 2013 Information Security for South Africa - Proceedings of the ISSA 2013 Conference, 2013.
18. Pelc, Lecture Notes in Computer Science: Preface, 2005, p. 3499.
19. N. Sjelin, "Cyber-Physical Security," Cyber-Physical Security, pp. 161-183, 2017.
20. F. Skopik, "Designing a cyber attack information system for national situational awareness," Communications in Computer and Information Science, vol. 318 CCIS, pp. 277-288, 2012.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 12, December 2019

21. Y. Soupionis, "Demo abstract: Demonstrating cyber-attacks impact on cyber-physical simulated environment," 2014 ACM/IEEE International Conference on Cyber-Physical Systems, ICCPS 2014, p. 222, 2014.
22. R. Spousta, "Ocean data vulnerability to cyber manipulation and consequences for infrastructural resilience," in FTC 2016 - Proceedings of Future Technologies Conference, 2017.
23. V. Subrahmanian, The Global Cyber-Vulnerability Report, The Global Cyber-Vulnerability Report, 2015, pp. 33-46.
24. R. Van Heerden, "Major security incidents since 2014: An African perspective," 2018 IST-Africa Week Conference, IST-Africa 2018, pp. Page 1 of 11-Page 11 of 11, 2018.
25. R. Van Heerden, "Classification of cyber attacks in South Africa," in 2016 IST-Africa Conference, IST-Africa 2016, 2016.
26. B. Van Niekerk, "Suppression of cyber-defences," in 2016 IST-Africa Conference, IST-Africa 2016, 2016.
27. B. Von Solms, "Critical Information Infrastructure Protection (CIIP) and Cyber Security in Africa - Has the CIIP and Cyber Security Rubicon been crossed?," in Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, 2012.
28. J. Walker, "Cyber security for emergency management," in 2010 IEEE International Conference on Technologies for Homeland Security, HST 2010, 2010.
29. G. B. White, "The Community Cyber Security Maturity Model The Center for Infrastructure Assurance and Security The University of Texas at San Antonio," Sciences-New York, pp. 1-8, 2007.
30. Z. S. Zainudin, "Advanced Persistent Threats Awareness and Readiness: A Case Study in Malaysian Financial Institutions," Proceedings of the 2018 Cyber Resilience Conference, CRC 2018, no. 2013, pp. 1-3, 2019.
31. W. Zhao, "A collaborative information sharing framework for community cyber security," in 2012 IEEE International Conference on Technologies for Homeland Security, HST 2012, 2012.
32. L. Maglaras, "Cyber Security: From Regulations and Policies to Practice," pp. 763-770, 2019.
33. R. Abeyratne, "Legal Priorities in Air Transport," Springer International Publishing, 2019.
34. R. Abeyratne, "Legal Priorities in Air Transport," Legal Priorities in Air Transport, 2019.
35. M. Albahar, "Cyber Attacks and Terrorism: A Twenty-First Century Conundrum," Science and Engineering Ethics, vol. 25, no. 4, pp. 993-1006, 2019.
36. Y. S. Baker, "Analyzing security threats as reported by the United States Computer Emergency Readiness Team (US-CERT)," IEEE ISI 2013 - 2013 IEEE International Conference on Intelligence and Security Informatics: Big Data, Emergent Threats, and Decision-Making in Security Informatics, pp. 10-12, 2013.
37. T.A. Johnson. "Cyber-security: Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare. CRC Press Taylor and Francis group. New York. 2015.
38. Cybersecurity Framework [Online] https://www.nist.gov/cyberframework [Accessed on 11/01/2019]
39. ITU National Cybersecurity Strategy Guide. [Online] www.itu.int/ITUD/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf [Accessed On 2019-01-15]
40. G. Mukelabai. Cybersecurity Efforts in Zambia. ITU Regional Cybersecurity Forum for Africa and Arab States. [Online] www.itu.int/ITU-D/cyb/events/2008/lusaka/docs/mukelabai-caz-zambia-lusaka-aug-08.pdf [Accessed on 22/06/2019]
41. Walls, Perkins E, Weiss J. Definition: "Cybersecurity", G00252816. Gartner Inc.; 013. [Google Scholar] [Accessed on 12/03/2019]
42. D. Galinec. The Ministry of Defence of the Republic of Croatia, Zagreb, Croatia Correspondence. Darko Možnik & Boris Guberina Cybersecurity and Cyber Defence: National Level Strategic Approach. Journal for Control, Measurement,Ele ctronics, Computing and Communications. Volume 58, 2017 - Issue 3 [Online] http://orcid.org/0000-0003-4465-6143 [Accessed on 06/06/2019]
43. R. Kaiser. The birth of cyberwar. Political Geography, Volume 46, May 2015, p11-20
44. M. Robinson, K. Jones, H. Janicke. "Cyber warfare: Issues and challenges Computers & Security", Volume 49, March 2015, Pages 70-94
45. S. Peter. Cyber resilience preparedness of Africa's top-12 emerging economies International Journal of Critical Infrastructure Protection, Volume 17, June 2017, p49-59
46. J. A. Bullock, G. D. Haddow, and D. P. Coppola. Book chapter 8: Cybersecurity and Critical Infrastructure. Protection Homeland Security (Second Edition), 2018, p189-226
47. P. Shakarian, J. Shakarian, and A. Ruef. Introduction to Cyber-Warfare: A Multidisciplinary Approach. Elsevier. New York. 2013.