Cyberterrorism Definition Patterns and Mitigation Strategies: A Literature Review

Israa G. SEissa[1], Jamaludin Ibrahim[2], Nor-Zaiasron Yahaya[3]

International Islamic University Malaysia

Abstract: ***This paper aim to contribute to the body of knowledge on cyber terrorism, improves awareness of cyber terrorism definition, boundaries, potential targets, crime patterns and effective mitigation strategies through analysis of relevant literature on the issue produced in recent years. It details the definitional origins of the concept and It looks at motivational factors and level of destruction necessary to classify a cyber-attack as cyberterrorism. The second sections is devoted to literature distinguishing cyberterrorism from hacking and cybercrime. Section three details the stages of a cyber attack, Section four lists the types of infrastructure targeted for cyber terrorists and Section five focuses on mitigation strategies.***

Keywords: Cyber Terrorism; Targeted attacks, Cyber Security; People, Process, Technology; Mitigation Strategies

1. Introduction

The UK Government predicted that by 2015 interconnected electronic devices would outnumber living humans [1] The average of computing capacities of homes computers by 2030 would be would be four thousand times greater than those of the machines available today [2].One of the central characteristics of the Information Age is connectivity.

The advances and development in computer technology coupled with wide availability of low cost, effective development tools and the availability of free knowledge online have enabled cyber terrorists to evolve their methods and conduct attacks remotely causing damages to their intended targets. This presents new opportunities to individuals and groups willing to involve themselves in illegal activity to further their shared goals, beliefs and agenda unseen and oftentimes undetected via cyber space, thereby creating new varieties of criminal threats. Spawning cyber terrorism; the use of cyberspace to carry out activities classified "terroristic". Cyber terrorists are able to perpetrate attacks through cyber-space and the virtual world, converging the physical world and cyber space [3]. Heartened by the diminished inherent threat of capture due to the distance between theme and their victims and the difficulty of tracing back the attack to them.

Interconnectivity has become central to government offices, critical infrastructures, (telecommunication networks, finance, transportation, and emergency services)as well as culture and education[4]. A variety of critical private, governmental, national, and military infrastructures can be vulnerable to cyber-attacks because they still rely on outdated conventional security solutions rather than a comprehensive, sophisticated cyber protection [5]. Cybercrimes, Cyber Terrorism and Cyber Warfare are all prevalent topics in the cyber security domain. Physical terrorism and cyber terrorism share some key elements and a common goal, namely terrorism. However, Cyber terrorism remains a vague concept with plenty of debate over its precise definition, aims, risk factors, characteristics, and preventive strategies [6].Cybercrime and Cyberterrorism are oftentimes used interchangeably, or the term Cybercrime may be used to include cyber terrorism, therefore blurring the distinction between them, especially to the general public. Cyber attacks are still listed as one of the highest priority risks to national security globally [7, 8].

2. Literature Review

Despite the inherent advantages, the dependence on information technology has left nations and society much more vulnerable to cyber attacks such as computer intrusions, scrambling software programs, undetected insider threats within the network firewalls, or cyber terrorists. A decentralized patchwork of systems that ensures relative anonymity, the Internet was designed as a benign venture of information exchange, making it inherently insecure and ill-equipped to trace attackers or to prevent them from abusing the intrinsic openness of the cyber space [4].

In a survey completed by 118 researchers working in 24 countries across six continents Jarvis & Macdonald, (2015) have found that, a majority of researchers agree that a precise definition of cyberterrorism is necessary for academics and policymakers. The debate however lies around what this exact definition is; further highlighting the need for a universal definition of this multijurisdictional problem for policymakers and researchers alike. The definition should, pin down the core characteristics or principal of the concept; and, the range of actual or potential scenarios to which the term cyber terrorism can be applied.[9] Defining cyberterrorism is made even more difficult by the abstract nature associated in understanding how certain incidents occur in cyberspace.

1.1 Definition

Barry Collin coined the term "Cyberterrorism" in the 1980's. There is still no agreement within the international community as to which exact cyber activities constitute as cyberterrorism [10].

In Denning's Testimony before the Special Oversight Panel on Terrorism [11] she made the following statement on cyberterrorism:

Cyberterrorism is the convergence of terrorism and cyberspace. It is generally understood to mean unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, plane crashes, water contamination, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyberterrorism, depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not.

Section 1 of the UK Terrorism Act 2000 [12] within subsection (2) defines “terrorism” to mean

> the ‘use or threat’ of action where— the use or threat is designed to influence the government or to intimidate the public or a section of the public, and the use or threat is made for the purpose of advancing a political, religious or ideological cause. For an action to fall under the terrorism category an action would have to; involve serious violence against a person, serious damage to property, endangers a person’s life, other than that of the person committing the action, creates a serious risk to the health or safety of the public or a section of the public, or is designed seriously to interfere with or seriously to disrupt an electronic system.

For an act to qualify, as ‘terrorism’ it must possess the three criteria; an **intent**, **motive** and **serious harm**. This means if a person threatensto commit a terrorist act he/she would fit the definition the same way as if he or she actually followed through with the threatened action.

According to NATO in 2008 they defined cyberterrorism as: a cyberattack using or exploiting computer or communication networks to cause sufficient destruction to generate fear or intimidate a society into an ideological goal. [13]In a 2011 report they used the term “digital (h)activism” to refer to cyber attackers who target those who do not share their political worldview [4]. They defined “Hactivism” as: social protest or expression of ideology by using hacking techniques.

A 2008 book by Council of Europe titled Cyberterrorism: the use of the internet for terrorist purposes (Terrorism and Law)suggests by definition all activities carried by a terrorist cell or individual over the Internet to be considered cyber terrorism. The United Nations Office on Drugs and Crime classified six ways in which the Internet can be used for terrorist activities: propaganda dissemination (recruitment, radicalization and incitement); financing; training; planning (through secret communication and open-source information); execution; and cyberattacks. [14]. For the purpose of this paper, we will focus on cyberterrorism attacks mitigation.

Hardware and software infrastructure, that collectively make up the Internet are still predominantly Western designed and produced. NATO Alliance unites nations with the most developed information and communication infrastructure; more than 50% of the world's Internet traffic transits the United States, this puts NATO and its Partner nationsat a higher risk of cyberattacks [4]. Depending on the perpetrators involved, and their motivation, cyberattackscan roughly be classified as acts of cybercrime, cyberterror, or cyber warfare.

1.2 Types of cyber attacks

Digital infrastructures have become strategic national assets, and now they are at risk. [8]from various types of cyberattacks. Thonnard et.al (2012) researched two common types of cyberattacks, targeted and non-targeted attacks on industrial systems.

Non-targeted malware attacks, which are random and have shown no evidence of selection of victim of the attack. The attacker hope to compromise any number of systems regardless of the identity of the systems presumably for monetary gains from sale or exploitation of information extracted from it. Targeted attacks on the other hand usually exhibits a higher degree of sophistication. Evidence shows that receivers of the attack are specifically selected; this may be because the attacker believes that their victim possess some highly valued information, or in hopes of using the compromised systems to launch attacks on other high value systems or individuals. Another feature distinguishing targeted attacks is that the malware is distinct from that used in non-targeted attacks.[15]

From the definitions of cyberterrorism we have reviewed it is agreed that it must be targeted and involve intent. The most common types of targeted cyber attacks are:

1) Malware short for malicious software, is any software code designed to gain unauthorized access to private computer systems, disrupt their operations, gather/delete sensitive data, or display unsolicited advertising. For example worms, trojan horses, and spyware.
2) DDos attacks take over a number of other computers (botnets) and use them without the knowledge of their owners to sendhugeamounts of network traffic to onemachine with the aim of overwhelm the target to a halt.
3) Stuxnets, a complicated Internet wormmay be the best knownworm exploiting industrial control systems (ICS). Using a combination of four zero-day exploits, command & control abilities, multiple propagation methods, and two stolen VeriSign driver certificates, plus a root kit it infectsICS hosts exclusively running Windows CC/Step [16].

Today, cities around the world use supervisory control and data acquisition (SCADA) systems to manage water, sewage, electricity, and even traffic lights and other critical infrastructure. ICS applications and protocols are insecure by design because theirvulnerabilities are easy to find. Adam Crain and Chris Sistrunk of Project Robus [17] found over 20 known and unknown vulnerabilities in DNP3 protocol stacks. The researchers tested the DNP3 protocol stack in the master of the control center. They wait for the master to send a request packet, to the PLC/controller and then sent back specially crafted response packets crashing the master.

Causing the control center to lose monitor and control ability of the SCADA network.

Existing deterrence models and mitigation methods confronting cyber terrorism have not managed to contain this threat [18].

3. Stages of a Targeted Cyber-Attack

Targeted cyber intrusions have no particular pattern of attack, nor is there a completely predictable sequence of events. An attack might be a onetime event that lasts for minutes, or a continued progression of intrusions lasting months or even years, taking advantage of multiple technical and human weaknesses, such as Web servers susceptible to code injection, unpatched browsers that unintentionally permit malware downloads or users who fall prey to opening malware infested email attachments [19]. Generally, it is useful to envision a targeted cyber intrusion in terms of stages. Thonnard et.al (2012) [15] observed that targeted attacks occur in several stages:

3.1 Reconnaissance

In the initial stage of an intrusion, an attacker takes the time out to gather information and understand their target using Social Engineering and Complacency, Email Phishing, creating a Watering Hole or tainting removable media. The intruder begins by looking up open-source information regarding the organization or government, scanning, gathering information on targeted networks, their systems, important personnel and email addresses associated with the target. The attacker(s) spend time documenting everything they find to gain an in depth insight of what is actually in use on that network and learning the security functionalities of devices to find vulnerabilities to exploit.

3.2 Scanning

The subsequent step is for the attacker to identify a weak entry point that allows access to the network, this could be poor judgment, unauthorized computer use, victims of social engineering, ignorance of or disregard for security policy. Once your network is compromised, inside the network, the intruder stealthily blends in with normal traffic, making detection extremely difficult. The enemy then begins by covertly deploying their cyber tools isolating security flaws within the network's vital links. The spying software will scan the environment probing computers, identifying vulnerabilities to create a cyber map of the network topography. This step can be accomplished using tools easily found on the Internet as well. Searching for vulnerabilities is usually a slow process that could last months at times, depending on how big the network is. [20]

3.3 Arbitrary code execution

Cyber criminals can remotely create rogue access points, or backdoors throughout your network install malicious software such as root kits, remote access Trojans (RAT), and implanting keystroke logging software to grab passwords to higher privileged accounts on your network and obtain the keys that will allow them access to all parts of the network. Having obtained a list of additional computers on the compromised network, the attacker begins to spread.

3.4 Access and Escalation

Now that the attacker has gained unrestricted access across the target network, they will attempt to move laterally spreading and establishing persistent presence. Some intruders hide in the deepest areas in the network and lay dormant coming and going as they please. Others may choose to look around the network to find the key pieces they are really after to complete their mission such as vital information, sensitive data, intellectual property or platform control systems degrading or disrupting network activity at whim.

3.5 Data Collection, Exfiltration, and exploitation

By this stage, integrity of the network has been fully compromised. Once an attacker determines they have created reliable network access, they are now able to alter sensitive data or move it out to any desired location. The attacker can use the stolen data for other malicious attacks or leak it to third party or the Internet. The ultimate objective of their mission is achieved and by this point It is usually too late for the breached entity to defend itself.

3.6 Clean up

The final step is not taken by all intruders, some merely disconnect, unconcerned with the victim eventually finding out what happened or wanting to leave a calling card behind to gloat over their achievement.. Highly skilled attacker attempt to rid all systems in the network of any forensic trail of evidence pointing to a breach. They will delete/overwrite data, remove implanted files, clean up event logs, deactivate alarms, roll back software updates, delete backups or erase hard drives. They will do their best to conceal or erase all traces that the incident ever occurred making it seem as a computer glitch leaving behind hidden backdoors they can return to and exploit the systems further whenever they want.

4. Infrastructure at Risk

4.1 Government Cyber and Physical Infrastructure

This type of cyber attack is usually advanced as it requires and attacker to bypassing strong network protections. This type of attack is targeting military, federal, or civilian government’s information technology services, infrastructure, functions, operations, systems and capabilities. The treat may come from outside actors or, an insider with sufficient misusing their authorized access rights to bypass network security [21].

In a 2011attack a Pakistani Hacker group, defaced the White House and the US Air Force Networks among several other US government websites. Georgian and Estonian e-government facilities faced an attack that rendered the government infrastructures useless [22]. These are only a few examples of the threat landscape facing government oriented cyber system.

4.2 Critical National Infrastructures

USA Patriot Act of 2001, states that critical infrastructure is “systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.”Critical infrastructure industries are enticing targets for cyber criminals because they host valuable confidential information and personally Identifiable Information (PII) about consumers [23]. The greatest risk to these organizations is the likelihood of cyber attacks on their computerized industrial control systems (ICS) intended to immobilize a company’s daily operations.

An example would be the 2010 malicious Stuxnet attack on Iranian nuclear centrifuges, which was designed to sabotage Iran's nuclear program with what would seem like a long series of unfortunate accidents [24] setting them back two years. Shamoon (Disttrack), a modular computer virus, was used in 2012 in an attack on 30,000 Saudi Aramco workstations, causing the company to spend a week restoring their services. [25]Others attacks include the Maroochy water and sewage system in Australia, in 2008, a cyber attack was launched against an oil pipeline in Turkey [26].Most recently, we have seen reports of multiple attacks on the power grid in Ukraine [27].

4.3 National/Social Identity

Attcks meant to mislead intimidate or defraud individuals and promint figures would fall under this section. The 2014 South Korean breach, where Crucial personal data like identification numbers, addresses and credit card numbers of nearly 20 million (40% of the country’s population) people were all stolen.epitomizing the seriousness of cyber attacks [28].

4.4 Private Industry organizations

Private entities are at a high risk of cyber attacksThe Titan Rain Malware, an example of cyber Espionage, was used to steal data from computers and networks belonging to different private organizations [18]. Cyber terrorism has been used to sabotageprivate industry sector organizations such asPayPal, MasterCard, Visa. Even prominent tech-savvy corporations are no longer immune. Reported list of cyber attack victims include Google, RSA, Sony, Lockheed Martin, PBS, Epsilon and Citibank as well as some security companies, defense contractors and some of the best in technology [28].In one of the biggest attacks in 2014, Sony Pictures Entertainment Company discovered its entire computer system had been hacked by an organization called Guardians of Peace. Several others have followed in 2015 and 2016 [29].

5. Mitigation Strategies

Like any other crime, cyber terrorism cannot be completely eradicated, but a number of effective mitigation strategies can be employed in attempts to combat and reduce any damage it may inflict on computerized systems. Cyber security goes far beyond investing in the latest hardware and software. International Telecommunication Union (ITU) defines cyber security as: The collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets… [28].

Primarily, cyber security needs to be viewed as a business matter. Meaning top-level management is accountable for ensuring the organization’s cyber security strategy meets business objectives and is taken on as a strategic risk. Smittlin and Munns (2010) “organizations should perform security risk assessments that employ the enterprise risk assessment approach and include all stakeholders to ensure that all aspects of the IT organization are addressed, including hardware and software, employee awareness training, and business processes.”[29]Board level discussions of cyber risk should include Risk identification, avoidance, acceptance, mitigation and risks transfer (e.g. through cyber insurance), in addition to assessing precise plans relating with each approach.

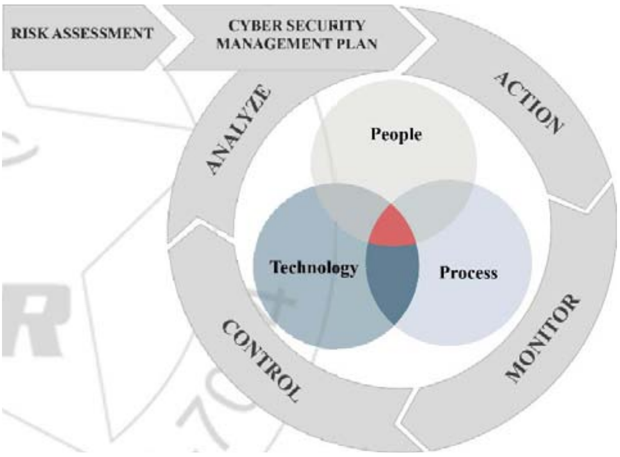

Figure 1: Comprehensive Cyber Security Management

Therefore, we can extract three central areas for an effective cyber security strategy, which are people**,** processes and technology. This section elaborates in more detail how those domains effect one another and mitigation strategies that address all three areas.

There exists obvious interdependencies between people, processes and technology. For example, deploying a firewall software requires staff skill and needs to be managed by a process. Organizations that fail to understand this intersection will not survive the ever-growing offensive of cyber attacks

Furthermore, merely trying to prevent an attack is no longer a solution. Organizations need to be ready to repel, respond to, and recover from a range of possible attacks. The only way accomplish this is if technology, people, and processes are all considered in the mitigation strategy.

5.1 Process

Efficient processes are vital to the implementation of an effective cyber security strategy they outline and detail how various organizational activities, procedures, roles and instructional documents are used to mitigate risks to an organization's information. Effective processes continually assess monitor risks outlined in the security strategy ensuring appropriate mitigating controls are implemented or improved as needed. implementation of an information security management system (ISMS) [30].

Adopt a Cyber Incident Response Plan and Employee Reporting Mechanisms so that the Chief compliance officer is promptly notified of all cyber attack attempts and can swiftly respond. All personnel should be aware of the possibility of cyber attacks and organizational assets most likely to be targets of such attacks. Every organization should develop a written cyber incident response plan customized for its particular circumstances. The plan should identify cyber attack scenarios and set out appropriate responses for each scenario. Generally, it should address the following basic modules: Response team, Reporting, Initial response, Investigation, Recovery and follow-up, Public relations, and Law enforcement procedure [31].

5.2 People

Organizations have traditionally focused on technical and procedural security measures to implementing information security solutions. Forgetting that the human factors are the most vulnerable part of a system [32]. Managing information security risks depends immensely on forming an effective and convincing Security Awareness (SA) culture. Effective cyber security requires that users be aware of and adhere to available security measures and mandates outlined in their respective organizations' ISMS policies and mandates [30].

Human factors, such as negligence and personal gain, or lack of motivation can adversely affect system security and integrity. For example, strict security policies that require employees to create strong complex password, or periodically expiring passwords may lead some staff to jot down their passwords and leave it in plain view. This opens a gate for intruders to the organizations' network. [30]

1) Four steps to addressing the people aspect 1) Motivating staff to be more inclination to participate in security policies. 2) Inclusion of all stakeholders in the process. 3) Individual Roles and responsibilities for various personnel are clearly defined. Last but not least 4) Training to deliver all necessary basic skills and knowledge to all parties. [30, 32]Staff awareness and training programs need to address two key levels of stakeholders:
2) **Technical** staff must update their cyber security skills, and poses broad competencies and qualifications [33]. Planning and executing an effective cyber security strategy is a complex activity that requires specialist knowledge. Poorly trained security management personnel can consequently result in inadequate security risk management and the implementation of cyber security strategies that fail to work. In addition, an organization's ability to respond to and recover from data breaches will also depend on the competency of technical staff.
3) **Non-technical** staff must have full awareness of their role in preventing and reducing cyber threats. If executed efficiently, SA programs will improve communication among different teams on various levels of the organization aiding the organization identify potential security problems, help all stakeholders understand the consequences of poor system security practices, assuring reliable roll-out of security procedures.

5.3 Technology

An effective cyber security program requires identification of cyber risks and selection of appropriate control measures that prevent or mitigate the impact of those risks. Technology plays a key role in an effective cyber security of any organization.

The consortium led by CSI's Center for Strategic and International Studies (CSI) has developed a set of 20 Critical Security Controls. The Twenty Critical Security Controls are derived from the most common attack patterns highlighted in the leading threat reports and vetted across a very broad community of government and industry practitioners. They have been widely adopted across the US Federal Government as well as by the UK's Centre for Protection of the National Infrastructure (CPNI) [34]. The Australian government has released a report containing a comprehensive list of targeted cyber intrusions and mitigation strategies [35]

The UK Government's Ten Steps to Cyber Security framework [36] summarizes 10 vital technical control measure addressing the role of people, processes and technology in systems security that should be considered for an effective cyber security strategy. They are:

1) An information risk management regime supported by top management
2) Secure home and mobile working
3) User education and awareness
4) User privilege management
5) Removable media controls
6) Activity monitoring
7) Secure configurations
8) Malware protection
9) Network security
10) Incident management

6. Conclusion

Cybercrime, no matter how it is defined or classified can have devastating effectson computerized networks. Until universally effective solution is found for this universal problem, the strength of a cyber-security management regime will depend on an information security management system that stresses comprehensive cyber risk assessment that considers all possible threats within an organization's domain this includes internal and external threats. Enforcement of ISMSs that address people, processes, and technologies as well as following best security practices, government guidelines and mandates for system security should help reduce cyber intrusion incidences.

References

[1] UK-Government, "A Strong Britain in an Age of Uncertainty: The National Security Strategy," The Stationery Office, Norwich, 2010.
[2] M. Kalkuhl, "IT security in 2030 – only humans will be the same," AO Kaspersky Lab., Moscow, 2012.
[3] D. A. Simanjuntak, H. P. Ipung and C. lim, "Text Classi-fication Techniques Used to Facilitate Cyber Terrorism Investigation," in Proceeding of Second International Con-ference on Advances in Computing, Control, and Tele-communication Technologies (ACT 2010), Jakarta, 2010.
[4] Lord Jopling UK NATO General Rapporteur, "171 CDS 11 E rev. 1 final InformationS And National Security General Report," NATO Par l iamentary Assembly International Secretariat, Brussles, 2011.
[5] M. A. A. &. C. E. Dogrul, "Developing an International Cooperation on Cyber Defenseand Deterrence against Cyber Terrorism.," Tallinn., 2011 .
[6] DCSINT, "Handbook No. 1.02, Critical Infrastructure Threats and Terrorism," US Army Training and Doctrine Command, Fort Leavenworth, K ansas, 2006.
[7] World Economic Forum , "Global Risks 2015 10th Edition," World Economic Forum , Geneva, 2015.
[8] NATO, "173 DSCFC 09 E bis - NATO and Cyber Defence," NATO, Brussles,Belgium, 2009.
[9] L. Jarvis and S. Macdonald, "What Is Cyberterrorism? Findings From a Survey of Researchers," Terrorism and Political Violence, vol. 27, no. 4, pp. 657-678, (2015).
[10] NATO, "171 CDS 11 E rev. 1 final - Information and National Security," 09 11 2011. [Online]. Available: http://www.nato-pa.int/default.asp?SHORTCUT=2589. [Accessed 17 12 2016].
[11] D. Denning, "“Cyberterrorism”, Testimony before the Special Oversight Panel of Terrorism Committee on Armed Services, US House of Representatives," 23 05 2000. [Online]. Available: https://pdfs.semanticscholar.org/7fdd/ae586b6d2167919abba17eb90e5219b7835b.pdf. [Accessed 17 11 201].
[12] UK Gov, "2000 CHAPTER 11," 21 7 2000. [Online]. Available: http://www.legislation.gov.uk/ukpga/2000/11/pdfs/ukpga_20000011_en.pdf.
[13] NATO, "Cyber defence concept MC0571," NATO, Brussels, Belgium, 2008.
[14] UNoDC, "The Use Of The Internet For Terrorist Purposes," United Nations Office On Drugs And Crime, Vienna, 2012.
[15] O. Thonnard, L. Bilge, G. O’Gorman, S. Kiernan and M. Lee, "Industrial Espionage and Targeted Attacks: Understanding the Characteristics of an Escalating Threat," in Research in Attacks, Intrusions and Defenses, Amsterdam, The Netherlands, 2012.
[16] M. M. Combs, "Impact Of The Stuxnet Virus On Industrial Control SYSTEMS," 2012. [Online]. Available: http://guap.ru/guap/nids/pdf_2012/combs.pdf. [Accessed 29 11 2016].
[17] I. A. Siddavatam and F. Kazi, "Security Assessment Framework for Cyber Physical Systems: A Case-study of DNP3 Protocol," in IEEE Bombay Section Symposium (IBSS), Bombay, 2015.
[18] S. Macdonald, L. Jarvis and T. Chen, "A Multidisciplinary Conference on Cyberterrorism Final Report," The cyber terrorism project, Swansea, 2013.
[19] Microsoft, "The Defence Signals Directorate Top 4 Mitigations Against Cyber Intrusion An Implementation Guide for Project Managers," Microsoft Corporation, 2012.
[20] M. B. Line, A. Zand, G. Stringhini and R. Kemmerer, "Targeted Attacks against Industrial Control Systems: Is the Power Industry Prepared?," SEGS '14 Proceedings of the 2nd Workshop on Smart Energy Grid Security, vol. 1, no. 1, pp. 13-22 , 2014 .
[21] C. Wilson, "Cyber Threats to Critical Information," in Cyberterrorism: Understanding, Assessment, and Response, New York, Springer, 2014, pp. 123-136.
[22] M. Dawson, M. Omar and J. Abramson, "Understanding the Methods behind Cyber Terrorism," in Encyclopedia of Information Science and Technology, Third Edition, Hershey, Information Science Reference (IGI Global), 2015, pp. 1539-1549.
[23] B. Boeck, "Cyber Attacks and Critical Infrastructure," Lockton companies, Kansas city, 2016.
[24] J. P. Farwell and R. Rohozinski, "Stuxnet and the Future of Cyber War," Survival, p. 23–40, 2011.
[25] C. Bronk and E. Tikk-Ringas, "The Cyber Attack on Saudi Aramco," Survival Global Politics and Strategy , vol. 55, no. 2, pp. 81-96 , 2013.
[26] S. Johnsen, "Mitigating Emergent Vulnerabilities in Oil and Gas Assets via Resilience," in Mitigating Emergent Vulnerabilities in Oil and Gas Assets via Resilience, Springer International Publishing, 201, pp. 43-61.
[27] ICS-CERT, "Alert (IR-ALERT-H-16-056-01) Cyber-Attack Against Ukrainian Critical Infrastructure," 25 02 2016. [Online]. Available: https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01. [Accessed 04 11 201].
[28] G. Dhillon, "The Changing Faces of Cybersecurity Governance: What to do before and after a cybersecurity breach?," Kogod Cybersecurity Governance Center (KCGC)., 2016.
[29] F. Wamala, "ITU National Cybersecurity Strategy Guide," ITU, 2011.
[30] ITU-T, "Rec ITU-T X.1500 SERIES-X: Data Networks, Open System Communications And Security Overview of cybersecurity information," International Telecommunication Union, Geneva, 2012.
[31] R. Schmittling and A. Munns, "Performing a Security Risk Assessment," ISACA Journal, pp. 1-7, 2010.
[32] R. Alavi, S. Islam and H. Mouratidis, "A Conceptual Framework to Analyze Human Factors of Information Security Management System (ISMS) in Organizations," in Human Aspects of Information Security, Privacy, and Trust Volume 8533 of the series Lecture Notes in Computer Science, Switzerland, Springer International, 2014, pp. 297-305.
[33] V. Farhat, B. McCarthy and R. Raysman, Cyber Attacks: Prevention and Proactive Responses, Practical Law Publishing Limited and Practical Law Company, 2011.

[34] M. Choi, Y. Levy and H. Anat, "The Role of User Computer Self-Efficacy, Cybersecurity Countermeasures Awareness, and Cybersecurity Skills Influence on Computer Misuse," in Proceedings of the Eighth Pre-ICIS Workshop on Information Security and Privacy, Milano, 2013.

[35] Z. Tu and Y. Yuan, "Critical Success Factors Analysis on Effective Information Security Management: A Literature Review," in Twentieth Americas Conference on Information Systems, Savannah, Georgia, 2014.

[36] CIS, "The CIS Critical Security Controls for Effective Cyber Defense," Center For Internet Security, 2016. [Online]. Available: https://www.sans.org/critical-security-controls. [Accessed 04 11 2016].

[37] Defence Signals Directorate (DSD), "Strategies to Mitigate Targeted Cyber Intrusions – Mitigation Details," The Australian Signals Directorate (ASD), Sydney, 2014.

[38] UK National Cyber Security Centre(NCSC), "10 Steps: Executive Summary," 08 Aug 2016. [Online]. Available: https://www.ncsc.gov.uk/guidance/10-steps-executive-summary. [Accessed 15 Nov 2016].