Impact of Cyber Threats to Nuclear Facility

Erasto Kayumbe
ICT and Statistics Unit, Tanzania Atomic Energy Commission
Arusha, Tanzania
Email: kayumbe [AT] yahoo.co.uk

Lucy Michael
Institute of Social Work
Dar es salaam, Tanzania
Email: lucymikel3 [AT] gmail.com

Abstract— **International community has been traditionally focusing on physical threats to facilities and pass by the threat of a cyber attack on a facility. All the same, due to the growing threat posed by cyber attacks; cyber security is becoming indispensable component of nuclear facilities and it is setting up itself as a main concern for facility operators and national regulators. Consequently, ensuring the security of nuclear facilities is a considerable element, which gears at avoiding theft of nuclear materials and sabotage. For that reason, this paper was set to examine impact of cyber threats to nuclear facility. Specifically, the paper has examined cyber threats, cyber threats to nuclear facility, impact of cyber threats to nuclear facility. It is concluded that cyber threat to nuclear facility is growing despite numerous effort taken to offset the problem. Thus, there is a need either to design or improve available cyber threat mitigation procedure in order to tone down the problem.**

Keywords-- Cyber, Threat, Security

I. INTRODUCTION

Cyber is a prefix that stand for computer and electromagnetic spectrum related works. The cyber domain consist of the Internet of networked computers, cellular technologies, space-based communications and fiber-optic cables (Nye and Joseph, 2011). A cyber threat is an activity planned to cooperate the security of an information system by changing the availability, integrity, or secrecy of a system or the information it contains. Cyber threats are tremendously growing and are exploiting capabilities created by the modernization of the power systems (ENISA, 2013). The cyber threat comes in various shapes, sizes, and forms. The term cyber security implies a wide range of issues and solutions connected to protecting residential subscribers, communications service providers (CSPs) and business customers from malicious harmful content and internet activity. Cyber threat actors are groups, states or individuals who, with malicious intent, aim to take benefit of vulnerabilities, low cyber security awareness and technological developments to gain unauthorized access to information systems. Enhanced threat scenario leads to the possibility of occurrences of cyber terrorism as a means of attacking state's critical infrastructures (IAEA, NSS, 17).

Malicious cyber activity is a security challenge facing many organizations across public and private sectors (Australia's cyber security strategy, 2016). The possible methods of a cyber attack on a nuclear infrastructure may include methods like: Exploiting an insider (insider threat); Social engineering method; and Supply chain contamination method (Dilipraj, 2019). Hence, several key systems like monitoring and Process Control Systems (PCS), Control Systems (DCS), Supervisory Control, Distributed and Physical Protection Systems (PPS), Data Acquisition (SCADA) that function on cyber resources are vulnerable to cyber threats (Dilipraj, 2019). Following this, high technology cyber possessions are employed in the nuclear infrastructure such as nuclear power plants Cyber attacks on civilian nuclear facilities can be take a form of three broad categories: access control systems, those that target business networks, and industrial control systems (ICS) - including security and safety systems. In the growing threat scenario, the likely occurrences of cyber terrorism as a means of attacking a state's vital infrastructure has encouraged a number of national authorities to plan defenses and issue new regulations. Such regulations establish computer security requirements which affect nuclear facilities at different levels and at different stages of operation (IAEA, NSS 17).

II. PROBLEM STATEMENT

Although the protection of important infrastructure is a pillar of the cyber security plan of any government, cyber threat to nuclear facility is tremendously growing. Cybercriminal, state-sponsored hackers, and cyber terrorists is hitting anyone, any place an in anytime. The attached nuclear facilities across the world is causing serious damage to the entire population. Due to that time to time measuring the impact of cyber threat to nuclear facility is necessary. The motive for the focus on cyber threats is due to the fact that it is the most significant new key elements that have entered the nuclear security arena in the last decades. Additionally it is quickly gaining prominence and importance due to growing reliance on digital tools and to game-changing events. Following this after several years in which cyber attack at nuclear facilities has grown up it is right time now to try to capture its impact (Dagoumas, 2019).

III. SCOPE AND METHODOLOGY

The primary aim of this paper was to provide guidance specific to nuclear facilities on implementing security programme. This paper provides advice on evaluating present programmes and procedures. Given limited time and resources available the sources of data has been desk study review and included; books, journals, papers, reports some cutting across the World and others focusing International Atomic Energy Agency (IAEA) and United Republic of Tanzania in particular Tanzania Atomic Energy Commission. Also, this paper is supported by personal observation and observation gathered from other people.

IV. CYBER THREATS

Computers and electronic controls play a part in all civil nuclear facilities in design, commissioning, and operation (Department for Business, Energy & Industrial Strategy, 2017). Cyber threats come from either internal or external attack (Jaccard, et al., 2013). While external attack come from cyber criminals, internal attack come from inside threats such as employees (Jaccard, et al., 2013). The main cyber threats are robots, which allow an unauthorized user to control the compromised computer for a variety of malicious purposes (DHS 2009). There are

other ten common types of cyber threats named malware, phishing, spear phishing, man in the middle, trojans, ransomware, denial of Service attack or Distributed Denial of Service Attack (DDoS), attacks on IoT Devices, data Breaches and malware on Mobile Apps. Cyber threats are likely to be harmful than physical threats (Ossip, 2017). Cyber threats seems to be equal to cybercrime. The term cyber threats describe violence, which include non-state actors, which can involve disruptions of critical infrastructures or politically disruptive acts (Ossip, 2017). Since internet users are not expected to discover safety risks and threats by themselves, it is advisable to increase personal awareness of the cyber threats (Ossip, 2017).

V. CYBER THREATS TO NUCLEAR FACILITY

There are two broad types of nuclear device that are gun-type and implosion-type. While gun-type can be made from enriched uranium, implosion-type are sophisticated devices made from HEU or separated plutonium (SP) (International Panel on Fissile Materials (2015). Horrible cyber capabilities cause serious security challenges, in particular to the nuclear domain (Boulanin and White, 2014). The International Atomic Energy Agency (IAEA) has listed three risk associated with cyber attacks on civil nuclear facilities that are cyber attack that corrupts a civil nuclear facility's command and control system; an act of cyber sabotage and an act of cyber espionage (Donovan 2015; Boulanin and White, 2014).

Computers has raised a new threat that cyber-attacks can conduct to nuclear facility (Gartze and Lindsay, 2017). Under this scenario Donovan 2015) has called upon countries to see the importance of strengthening computer security at all levels that will guard against cyber threats, which affect nuclear security. Computer security is part of important aspect of nuclear security in the newly expanding application of digital systems (Boulanin and White, 2014). Yet there is misconception that cyber-attacks cannot take place if a computer is not connected to internet, intranet, WiFi or router (Zetter, 2014). This argument is false as cyber-attacks in some places have be carried out even without the internet (Zetter, 2014). It should be noted that since there is an expand of nuclear weapons which are linked to computers there is also an increase of a cyber against them (Boulanin and White, 2014).

Cyber attacks can retard nuclear facility operations as well as compromise critical components within the C&C structures. There are two main systems for security in any nuclear facility that are instrument and control security (ICS) and facility network security (FNS). Consequently, computer security is being recognized as a key component in nuclear security. Thus as technology move on, the use of computers and computing systems in all areas of plant operations is expected to increase (International Atomic Energy Agency, 2016). Therefore, computer systems used for physical protection, nuclear safety to mention few should be protected against cyber-attack, manipulation or falsification (International Atomic Energy Agency, 2016).

VI. IMPACT OF CYBER THREATS TO NUCLEAR FACILITY

There are several factors that determine vulnerability of nuclear plant, which leads to facility attack. To start with the design of the plant will determine the extent to which a nuclear plant is vulnerable to attacks. Other factor are organizational history of the plant, the technical operation of the plant, types of computers used in the plant, interaction of networks allowed by computers to mention few. Most of these attacks disturb supply in the facility, damage facilities, cause: delay hazard, risk adverse and risk reduction. Protecting nuclear facilities from damaging cyber-attacks is made more difficult by their complexity. A facility may include more than a thousand digital apparatus, including legacy systems without built-in security (Rudner, 2013). Older facilities are changing to digital systems that while often bringing bigger trustworthiness and safety, also turn out to be more vulnerable to cyber-attacks (Rudner, 2013). As the results the threats causes impacts to workers, the public or the environment (Department for Business, Energy & Industrial Strategy, 2017).

A. Business Networks

Attacking on business networks likely to cause theft of sensitive data that can be used to blackmail or financial gain. There are several cyber threats to business network. To mention few there are automated exploit of a known vulnerability whereby attacks try to exploit vulnerabilities in Windows and it occur when all necessary patches are not installed (ISO/IEC, 2011). Malicious HTML email attacks HTML email, which links to a malicious when the use click mistakenly the link on that malicious website (ISO/IEC, 2011). Reckless web surfing by employees likely to affect company network with bot clients (Ambroz, 2012). Employees surfing online using company computer can normally be put under malware attack (Yan et al., 2011). In web server compromise website cause vulnerability if its custom code is poor written leaving some security holes to be exploited by attackers. Regarding data lost on a portable device portable devices such as laptops always at a high risk of being stolen (Hoard, 2017). Concerning reckless use of wi-fi hotspots the attacker can monitor traffic of the victims and steal their valuable information (ISO/IEC, 2011). Attackers can also control business system and lay a groundwork for a next attack. Again the attacker can maneuver nuclear reactor control systems (Samani, and Mcfarland, 2015). Cyber attacker facilitate theft of nuclear materials, it they also act as sabotage resulting in radiological release (Rudner, 2013).

B. Access control systems

An attack on access control system can lead to the theft of nuclear material. An attacker can easily hack into a badge permission system with the intention of gaining access over restricted parts of a facility (nuclear material are kept) and negotiation materials accounting systems to hide the theft. Cyber attack can disable some of the physical protection measures like closed circuit television cameras (Quevenco, 2015).

C. Industrial control systems (ICS)

In this category the attack threats digital systems, which control sensors, heaters and valves. Again the attack can disable cooling systems that can lead to the release of radioactive material. The threats also affect system operators and market participants (Dagoumas, 2019). In industrial control systems reconnaissance attacks collect control system network information, plan the network architecture, and figure out the device distinctiveness that are model number, manufacturer, supported network protocols, system memory map and system address (Morris and Wei, 2013). There are many computer-based things in control systems (Cárdenas et al., 2011). Targeted attacks are the biggest threat to control system. These attacks are those where the miscreants know that they are targeting control systems tailor their attack strategy with the aim of injuring the physical system under control. Targeted attacks not in favor of control systems are not new. Cyber-attacks on industrial control system are cheaper, not constrained by distance, less risky for the attacker and are easier to replicate and coordinate (Cárdenas et al., 2011).

VII. CONCLUSION

Cyber threat to nuclear facility is gradually growing despite efforts taken to mitigate the problem. Lack of cyber security policies, procedures and training makes the situation worse. Yet, operators of nuclear facilities are not equipped to become aware of and act in response to cyber-attacks. Therefore, there is a need to develop or improve guidelines that will permit the measurement of cyber security risks in the nuclear industry, rising the awareness of the cyber threats among the sector. Experts in the nuclear industry could do with developing guidelines to measure cyber security risks by considering security and safety measures. This approach will in general prove effective against untargeted cyber-attacks.

REFERENCES

- Ambroz Milan (2012). Security Culture Impact on Security Excellence in a Company". Innovative Issues and Approaches in Social Sciences, vol.5, no.1:70-87, DOI:http://dx.doi.org/10.12959/issn.1855-0541.IIASS-2012-no1-art06

- Boulanin, V and White, T.O (2014). Cyber Threats and Nuclear Dangers. http://cnnd.anu.edu.au
- Cardenas, A.A; Amin, S, Lin, Z.S; Huang, Y.L; Huang, C.Y and Sastry, S (2011). Attacks Against Process Control Systems: Risk Assessment, Detection, and Response.
- Dagoumas A. (2019). Assessing the Impact of Cyber security Attacks on Power Systems. www.mdpi.com/journal/energies (Site visited on 11/6/2020).
- Department for Business, Energy & Industrial Strategy (2017). Civil nuclear cyber security strategy. www.gov.uk/beis (Site visited on 13/6/2020).
- DHS. 2009. Roadmap for Cybersecurity Research. Department of Homeland Security. [Internet]. Accessed 15 July 2013. Available from: www.cyber.st.dhs.gov/docs/DHSCybersecurity-Roadmap.pdf
- Dilipraj, E (2019). Challenges of Cyber Security to Nuclear Infrastructure. https://www.researchgate.net/publication/333420287.
- Donovan, J (2015). IAEA's Amano Calls for Strengthened Computer Security in a Nuclear World," IAEA, 01 June 2015, URL: https://www.iaea.org/newscenter/news/iaea % E2 % 80 %99s-amano-calls-strengthened-computer-security-nuclear-world, accessed on 24 June 2020.
- ENISA (2013). Smart Grid Threat Landscape and Good Practice Guide. 2013. https://www.enisa.europa.eu/publications/smart-grid-threat-landscape-and-good-practice-guide (Site visited on 8/6/ 2020).
- Gartze, E and Jon R. Lindsay (2017). Thermonuclear Cyber war", *Journal of Cybersecurity*, 3(1), 2017, pp. 37-47.
- Hoard, B (2017). 8M cell phones will be lost in '07 – how to back yours up, Computerworld, Jul. 2007
- International Atomic Energy Agency (2016). Conducting Computer Security Assessments at Nuclear Facilities. http://www.iaea.org/books.
- International Panel on Fissile Materials (2015). Global Fissile Material Report 2015: Nuclear Weapon and Fissile Material Stockpiles and Production.
- ISO/IEC 27005 (2011). Information technology — Security techniques — Information security risk management (second edition), Int'l Org. Standardization, 2007. Available:http://www.iso27001security.com/html/27005.html.
- Jaccard, J.J; Nepal, S and Guo, J. Y (2013). Cybersecurity threats in cloud computing. Australian Journal of Telecommunications and The Digital Economy, 1 (1):4.1 - 4.17.
- Morris, T and Wei G (2013). Industrial Control System Cyber Attacks. https://www.researchgate.net/publication/336586158.
- Nye, Jr., Joseph S. (2011). Nuclear Lessons for Cyber Security? Strategic Studies Quarterly 5(4): 18-38.
- Ossip, S.M (2017). Cyber threats and cybercrime – a disruption of human security? Master of Arts in International Relations, Leiden University.
- Quevenco, R., (2015). Secure Computer Systems Essential to Nuclear Security, Conference Finds, IAEA Office of Public Information and Communication, https://www.iaea.org/newscenter/news/secure-computer-systems-essential-nuclearsecurity-conference-finds
- Rudner, M. (2013). Cyber-threats to critical national infrastructure: An intelligence challenge. *International Journal of Intelligence and Counter Intelligence*, *26*(3), 453-481.
- Samani, R., and Mcfarland, C., (2015). Hacking the Human Operating System: The Role of Social Engineering Within Cyber security," McAfee Incorporated, http://www.mcafee.com/de/resources/reports/rp-hacking-human-os.pdf
- Schreier, F (2015). On Cyberwarfare", 2015, URL: https://www.dcaf.ch/sites/default/files/ publications/documents/OnCyberwarfare-Schreier.pdf, 25 February 2020.
- Yan, G., Chen, G., Eidenbenz, S., & Li, N. (2011). Malware propagation in online social networks: nature, dynamics, and defense implications. In *Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security* (pp. 196-206). ACM.