International Journal of ASRO
Volume 13, Number 03, pp.8-12
July 2022

ANALYSIS OF POTENTIAL ASYMMETRIC THREATS BASED ON CYBER SECURITY VULNERABILITY IN THE NEW RENEWABLE ENERGY INDUSTRY SECTOR

Joko Yulianto [1], Suyono Thamrin [2], Yusuf Ali [3], Richard Martin[4]

[1,2,3] Energy Security, Indonesia Defense University, Bogor, West Java

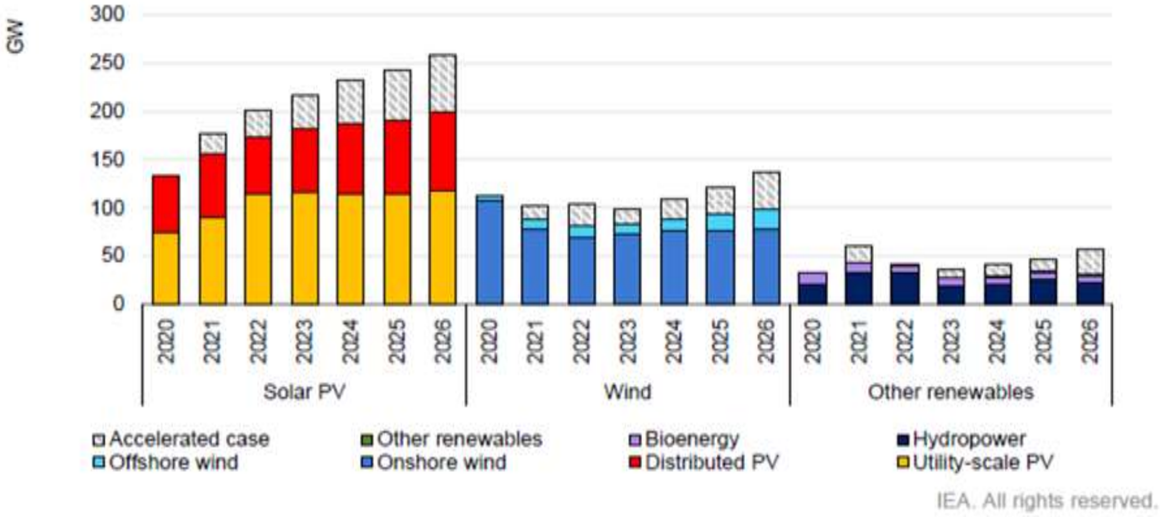
ABSTRACT

The start of this decade marks an important turning point in the passage from Society 4.0 to Industrial Era 4.0. All tiers of society are now able to adapt to technological advancements as a result of the changes in this era. It can lessen the distance between humans and future economic issues in Society 5.0, where humans are the primary component and are capable of producing new value through technological advancements. Although conflicts and wars have now entered a new era, the development of technology has an impact on these developments. There are many different, improbable, and unknowable threats that could materialize. These cyber threats have the ability to cause a nation to suffer significant losses. Cyberattacks against crucial state infrastructure, such as power plants, or on important national targets could have a significant influence in the future. High-tech renewable energy power plants that are connected to a vast distribution network can result in power outages or even global blackouts brought on by negligent parties or non-state actors if network security is not strengthened. Therefore, all nations must be able to plan for growth, create new units, and fortify their individual national defenses.

Keywords: *Cyber Security, Cyber Threats, Renewable Energy Sector, Asymmetric Warfare.*

1. INTRODUCTION

The globe had to produce renewable energy due to technological advancements during the last ten years. The International Energy Association (IEA) reports that Europe has seen a rise in renewable energy that has never been seen before. The requirement that each nation achieve net-zero emissions, whether slowly or fast, supports this. The creation of Renewable Energy must be standardized, and all ISO, SOP, and safety regulations must be followed in accordance with the producing industry as well as global agreements and EBT policies. According to the IEA (2020), the development of NRE in Europe is shown in Figure 1.



IEA. All rights reserved.

Figure 1. Global Renewable Energy Development

The renewable energy industry is important as countries seek to move away from fossil fuels, but the sector's continued growth must be managed with cyber security in mind as it has indicated the dangers of vulnerabilities in everything from power plants to smart meters that could be lost or lost. manipulation, this will disrupt the grid/microgrid of Renewable Energy. Energy providers, customers and policymakers, and governments must be open to the risks of cyber threats. Cyber threats are asymmetric or indirect and have the potential to threaten data and information security and harm state finances. Cyber threats to be overcome are classified as military operations other than war.

Military Operations Other than War aims to assist ministries/institutions and the police in overcoming threats that can harm and have an impact on state security and sovereignty. Therefore, an ideal Defense posture is needed to be able to ward off and mitigate cyber threats to the country's infrastructure, especially national vital objects such as new renewable energy and operating smart grid systems.

2. MATERIALS AND METHODS

2.1 Cyber Threat Analysis

The use of technology, procedures, and controls to defend systems, networks, programs, devices, and data against cyberattacks is known as cybersecurity. Cybersecurity strives to lower the risk of cyberattacks and safeguard sensitive information from virus-infected devices and programs that hack systems, networks, and other technology. The 5 types of cyber security are described as follows:

a. Critical Infrastructure Cybersecurity

Critical infrastructure is often more vulnerable to attack than others because SCADA (Supervisory Control and Data Acquisition) systems often rely on older software. Key service operators in the UK's energy, transport, health, water, and digital infrastructure sectors, as well as digital service providers, are bound by the NIS Regulations (Networks and Information Systems Regulations 2018). Among other provisions, national policies are required to implement technical security measures against vital national objects, agencies, ministries, and institutions to manage their data security.

b. Network Security

Network security involves addressing vulnerabilities that affect your operating system and network architecture, including servers and hosts, firewalls and wireless access points, and network protocols.

c. Cloud Security

Cloud security is concerned with securing data, applications and infrastructure in the Cloud.

d. Internet of Things Security

IoT security involves securing smart devices and networks connected to the IoT. IoT devices include things that connect to the Internet without human intervention, such as smart fire alarms, lights, thermostats, and other appliances.

e. Application Security

Application security involves addressing vulnerabilities that result from an insecure development process in the design, coding, and publishing of software or websites.

A new report by the defense and security think tank Royal United Services Institute (RUSI) has outlined some of the top cyber threat risks during the transition to renewable energy from fossil fuels. "Renewable energy offers a great opportunity for the UK to become more self-sufficient in energy production while mitigating the impacts of climate change. This transition must be made with cybersecurity in mind, recognizing the future cyber threats to society due to the massive digitization of the sector. ," said Sneha Dawda, a cybersecurity researcher at RUSI. This is also because renewable energy technology tends to be new, so it is still necessary to adapt and improve the renewable energy industry so that it is not vulnerable to cyber-attacks. The vulnerability of renewable energy technologies as a result of the threat of cyber-attacks is described as follows:

a. Cybersecurity is not a priority to be strengthened during the design phase for most of the renewable energy industries operating today.

b. The trend of the renewable energy industry is to use SCADA systems and low-cost/low-cost CCTV systems that are ready to use.

c. The main components are selected without considering Cybersecurity.

d. There are no policies or regulations to follow regarding cybersecurity in the renewable energy sector.

e. Buyers and Technical Advisors for the renewable energy industry tend not to check Cybersecurity from the transaction, installation, and settlement to acceptance.

f. One of the main concerns facing the renewable energy sector is the cybersecurity risk in the supply chain.

Renewable energy providers should take a more careful approach to the supply chain, Renewable energy operators should ask a lot of questions to suppliers/renewable energy industry parties, If necessary, periodic maintenance improvements should be made. Most energy companies around the world are increasingly encouraging customers to install smart meters and other sensors. However, smart meters and other IoT devices can be vulnerable to cyberattacks. This is because IoT has the potential to provide routes to networks and the ability to build botnets for cyber-criminals.

Executives of energy supply companies must be able to take tactical steps related to IoT because it is quite difficult for users to patch the weaknesses and shortcomings of IoT devices. There is a need for regulations and policies such as legislation related to design security to help improve cybersecurity and further research on risk mitigation strategies and policy-focused recommendations are needed.

2.2 Defense System Posture in Overcoming Cyber Threats

The National Defense System positions the National Army x as the main component to ward off military threats (physical threats) assisted with reserve components and supporting components, but apart from that, the National Army x is responsible for conducting War Military Operations and Military Operations Other Than War. this is based on National Defense Policy 2018.

The development of the national defense posture in dealing with cyber threats must be following and in line with the Minister of Defense Regulation No. 82 of 2014 concerning cyber defense guidelines. Based on Figure 2, the agency that is the leading sector related to cyber threats is the National Cyber Agency. National Cyber Agency will later cooperate with the National Police as law enforcers in taking further legal action after cyber security. Based on the nature of the threat, the National Army x is also responsible for anticipating this by creating units such as the National Forces Cyber Unit x which was formed on October 13, 2017.

Considering cyber threats that are increasingly advanced and threaten national vital objects/critical information infrastructure, information security and digitization in the field of state defense and the ministry of defense. in early 2022, National Forces Cyber Unit x collaboration with National Cyber Agency decided to form a small unit. This unit prevents and responds to information security incidents that are directly related to the national defense sector under the National Army x and the Ministry of Defense.

The use of Cyber Technology must be accompanied by the cyber defense as an effort to anticipate the threat of digital crime, such as attempts to break into the confidentiality of information, damage electronic systems, espionage, and hackers on National websites have occurred to the deactivation of the Instagram account of the Ministry of Tourism as well as various other unlawful acts committed by non-state actors or irresponsible persons. Taking into account the above, cyberspace needs to get proper protection to avoid the potential that can harm individuals, organizations and even the state. National Forces Cyber Unit x consists of implementing units including deterrence units, recovery units, aid units and enforcement units. In the future, there needs to be ongoing training related to cyber security and passwords.

3. RESULTS AND DISCUSSION

3.1 Research method

The research method used is a qualitative method with a literature study approach [32]. Literature study means using reading material as the main object of data [33], this research will produce information in the form of notes and descriptive data contained in the text that is researched exploratively [34].

Data collection techniques by utilizing various sources of information that can be validated and the reliability of the information can be measured (Literature Study). A limited search was conducted using the terms “Asymmetric Warfare”, “Cyber Security”, “New Renewable Energy Industry”, “Cyber Threats”, and “Defense System Posture”. Limited searches related to themes in English and Indonesian with a range of 2001 and 2022, The search results used range from scientific articles, research reports, reviews, anecdotes, proceedings, valid news and opinion pieces by the authorities with very good scientific backgrounds.

4. CONCLUSIONS

Based on the results of research and discussion that have been stated in the previous chapter, the conclusions generated in this study are as follows:

a. New and renewable energy has experienced unprecedented growth in Europe and any part of the world but behind its development lies serious threats, especially cyber-attacks. The threat of cyber-attacks on vital renewable energy objects was first felt by renewable energy projects in the United States. The company is called sPower. The agency owns power plants that utilize solar and wind power experiencing a series of broken connections between its main control centre and remote power generation sites.

b. The short and intermittent periods of downtime were allegedly caused by a Distributed Denial of Service (DDoS) attack. Because of the government's role in assisting regulatory and tactical policies such as designing security-related laws to help improve cybersecurity and further research on risk mitigation strategies and policy-focused recommendations are needed. The ideal defense posture is needed to deal with asymmetrical threats such as cyber-attacks that have the potential to harm individuals and the state.

ACKNOWLEDGEMENT

The authors greatly acknowledge the support from Indonesia Naval Technology College STTAL Surabaya Indonesia for providing the necessary resources to carry out this research work. The authors are also grateful to the anonymous reviewers and journal editorial board for their many insightful comments, which have significantly improved this article.

REFERENCES

Aghenta, L. O., & Iqbal, T. (2019). Design and implementation of a low-cost, open source IoT-based SCADA system using ESP32 with OLED, ThingsBoard and MQTT protocol. AIMS Electronics and Electrical Engineering, 4(1), 57-86.

Alabady, S. A., Al-Turjman, F., & Din, S. (2020). A novel security model for cooperative virtual networks in the IoT era. International Journal of Parallel Programming, 48(2), 280-295.

Alotaibi, I., Abido, M. A., Khalid, M., & Savkin, A. V. (2020). A comprehensive review of recent advances in smart grids: A sustainable future with renewable energy resources. Energies, 13(23), 6269.

Anggito, A., & Setiawan, J. (2018). Metodologi penelitian kualitatif. CV Jejak (Jejak Publisher).

Bedi, G., Venayagamoorthy, G. K., Singh, R., Brooks, R. R., & Wang, K. C. (2018). Review of Internet of Things (IoT) in electric power and energy systems. IEEE Internet of Things Journal, 5(2), 847-870.

Brangetto, P., & Aubyn, M. K. S. (2015). Economic aspects of national cyber security strategies. Brangetto P., Aubyn MK-S. Economic Aspects of National Cyber Security Strategies: project report. Annex, 1(9-16), 86.

Buchanan, B. (2020). The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics. Harvard University Press.

Calamanti, G. (2021). Security and Climate Change linkage: Analyzing the European discourse until the Defense Roadmap.

Cole, E. (2011). Network security bible. John Wiley & Sons.

Darmalaksana, W. (2020). Metode Penelitian Kualitatif Studi Pustaka dan Studi Lapangan. Pre-Print Digital Library UIN Sunan Gunung Djati Bandung.

Dutta, P., Choi, T. M., Somani, S., & Butala, R. (2020). Blockchain technology in supply chain operations: Applications, challenges and research opportunities. Transportation research part e: Logistics and transportation review, 142, 102067.

Fay, M., Hallegatte, S., Vogt-Schilb, A., Rozenberg, J., Narloch, U., & Kerr, T. (2015). Decarbonizing development: Three steps to a zero-carbon future. World Bank Publications.

Gunduz, M. Z., & Das, R. (2020). Cyber-security on smart grid: Threats and potential solutions. Computer networks, 169, 107094.

Hamzah, D. A. (2021). Metode Penelitian Kualitatif Rekontruksi Pemikiran Dasar serta Contoh Penerapan Pada Ilmu Pendidikan, Sosial & Humaniora. CV Literasi Nusantara Abadi.

Henrie, M. (2013). Cyber security risk management in the SCADA critical infrastructure environment. Engineering Management Journal, 25(2), 38-45.

Idris, A. M., Sasongko, N. A., & Kuntjoro, Y. D. (2022). Energy Conversion and Conservation Technology in Facing Net Zero-Emission Conditions and Supporting National Defense. Trends in Renewable Energy, 8(1), 49-66.

Idris, A. M., Sasongko, N. A., & Kuntjoro, Y. D. (2022). "AUKUS Cooperation in the Form of Australian Nuclear Submarine Technology for Stability in Indo-Pacific Region". International Journal of Research and Innovation in Social Science (IJRISS). 6(2), pp.745-750. DOI: https://dx.doi.org/10.47772/IJRISS.2022.6237.

IEA. 2021. Renewable 2021 Analysis and Forecast to 2026. International Energy Agency Report and Publication 2021.

Kammen, D. M., & Sunter, D. A. (2016). City-integrated renewable energy for urban sustainability. Science, 352(6288), 922-928.

Kementerian Pertahanan Republik Indonesia. 2017. Kebijakan Pertahanan Negara Tahun 2018. Kementerian Pertahanan Republik Indonesia

Khanna, M. (2021). COVID-19: A cloud with a silver lining for renewable energy?. Applied economic perspectives and policy, 43(1), 73-85.

Markopoulou, D., Papakonstantinou, V., & De Hert, P. (2019). The new EU cybersecurity framework: The NIS Directive, ENISA's role.

Overland, I. (2019). The geopolitics of renewable energy: Debunking four emerging myths. Energy Research & Social Science, 49, 36-40.

Peraturan Menteri Pertahanan Republik Indonesia NOMOR 82 TAHUN 2014 tentang Pedoman Pertahanan Siber

Plėta, T., Tvaronavičienė, M., Casa, S. D., & Agafonov, K. (2020). Cyber-attacks to critical energy infrastructure and management issues: Overview of selected cases.and the General Data Protection Regulation. Computer Law & Security Review, 35(6), 105336.

Pusat Penerangan Tentara Nasional Indonesia. 2022. Peresmian Military Computer Security Incident Response Team (Mil-CSIRT) TNI. https://tni.mil.id/video-607-peresmian-military-computer-security-incident-response-team-mil-csirt-tni.html.

Samarati, P., di Vimercati, S. D. C., Murugesan, S., & Bojanova, I. (2016). Cloud security: Issues and concerns (pp. 1-14). Chichester: Wiley.

Tahaei, M., & Vaniea, K. (2019, June). A survey on developer-centred security. In 2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW) (pp. 129-138). IEEE.

Vakulchuk, R., Overland, I., & Scholten, D. (2020). Renewable energy and geopolitics: A review. Renewable and Sustainable Energy Reviews, 122, 109547.

Walker, A., Desai, J., Saleem, D., & Gunda, T. (2021). Cybersecurity in Photovoltaic Plant Operations (No. NREL/TP-5D00-78755). National Renewable Energy Lab.(NREL), Golden, CO (United States).

Yan, Y., Qian, Y., Sharif, H., & Tipper, D. (2012). A survey on smart grid communication infrastructures: Motivations, requirements and challenges. IEEE communications surveys & tutorials, 15(1), 5-20.

Yannakogeorgos, P. (2021). Cyber Competition and Global Stability. In The Future of Global Affairs (pp. 223-246). Palgrave Macmillan, Cham.

Yergin, D. (2006). Ensuring energy security. Foreign affairs, 69-82.

Zaheeruddin, & Manas, M. (2015). Analysis of design of technologies, tariff structures, and regulatory policies for sustainable growth of the smart grid. Energy Technology & Policy, 2(1), 28-38.

Zaman, G., & Cristea, A. (2011). EU structural funds absorption in Romania: obstacles and issues. Romanian Journal of Economics, 32(1), 41.