Available online www.ejaet.com

European Journal of Advances in Engineering and Technology, 2021, 8(10):113-121

Research Article ISSN: 2394 - 658X

Cybersecurity for National Critical Infrastructure Safeguarding Against Cyberterrorism

Siva Krishna Jampani

Software Engineer

ABSTRACT

Cybersecurity for critical national infrastructure is crucial for ensuring the safety, resilience, and continuity of operation of the infrastructural systems that form the foundation of society. Transportation networks, utilities, energy systems, and communication frameworks are being threatened by sophisticated cyberterrorism threats in an increasingly digitized and networked world. New technologies like SCADA systems and IoT devices have significantly increased the attack surface of critical systems in recent years, which requires a holistic approach to cybersecurity. The article provides a summary of the rapid growth of cyber threats to critical infrastructure, identifies significant vulnerabilities, and outlines effective mitigation strategies. These case studies and best practices emanate from such sectors as energy, transportation, and public utilities; such dialogue determines the importance of public-private partnerships, coordinated response mechanisms, and international cooperation in strengthening resilience to cyberterrorism.

Keywords: cybersecurity, critical infrastructure, cyberterrorism, SCADA systems, national security, public-private partnerships, cyber risk management, resilience

---

INTRODUCTION

Critical National Infrastructure (CNI) is the backbone of modern society, comprising the systems and assets upon which the functioning of daily life depends. The list includes infrastructures like transportation, energy, water supply, and telecommunications—critical to the stability of both the economy and societal function. However, growing dependence on digital systems has placed these infrastructures at some unprecedented major risks to national security and public safety in regard to cyber threats such as cyberterrorism and cybercrime. Among them, the impacts of cyber terrorism are those most organized by using developed digital machineries against CNI, aiming at disturbing activities and spreading panic. Thus, energy infrastructure—the lifelines in the context of oil and gas systems—are major targets to ensure key supports of economic and societal activities [2][16]. Cyberattacks against Korea Hydro & Nuclear Power Co., in year 2014, further manifests the weakness of state-sponsored CNI cyberterror; Therefore, there comes into being a critical urgency for stringent cyber security schemes for this protection [8].

Emerging national and international policies is now putting more emphasis on the building up of resilience against such threats. Illustrative examples in this regard include those EU initiatives that stress collaboration in infrastructure protection through public-private partnerships and legislative frameworks to redress vulnerabilities [6][9]. Similarly, the creation of security protocols for SCADA systems is a very relevant factor in the reduction of risks within those critical systems of energy, transportation, and Watersectors [5] such efforts, cyber threats are becoming increasingly sophisticated, often outpacing available defensive measures. In order to counteract such challenges, innovative approaches are called for, such as the introduction of due diligence in cybersecurity and international cooperation to reinforce national security [11][18]. As research goes on, active involvement of public and private organizations in the actual deployment and upkeep of cybersecurity measures is important to ensure the resilience of CNI from Cyber terrorismand other related threats [6][14].This article provides an overview of the multi-dimensional challenges and emerging strategies for the protection of CNI from cyber threats, focusing on critical roles that collaboration, cutting-edge technology, and policy frameworks play in safeguarding these lifeblood systems.

LITERATURE REVIEW

Rudner, M. (2013): Discusses the rising concern about the threat of cyberattacks on critical national infrastructure and how they could paralyze significant services, including national security. The article underlines the importance of having comprehensive strategies and intelligence-sharing mechanisms to thwart such threats and ensure national defense preparedness. The author discusses cyber-terrorism as a tool used to destabilize critical infrastructure, elaborating on its strategic implications for global security. [1]

Kumar, V. S., Prasad, J., and Samikannu, R. (2018): Provide a description of the potential hazards of cyber terrorism for the energy industry and focus on critical infrastructure vulnerabilities. The authors critically review the existing security mechanisms set in place to ensure energy system protection and also present an integrated approach to mitigating cyber risks. The paper highlighted the need for enhanced cooperation between the public and private sectors to secure the energy infrastructure. [2]

Wilson, C. (2014): States that critical information infrastructure exposes many vulnerabilities that increase risks through cyber-attacks. According to him, cyber-terrorism has become a distressing threat to national security, and a more robust cybersecurity framework needs to be developed. International cooperation is necessary to combat cyber threats against critical information systems, as stated in this chapter. [3]

Mikacitit R., Mamic K., (2020): Discussess the increased threats of cyberterrorism to the critical infrastructure of Southeastern Europe. They highlight the need for coordinated prevention measures to be taken at both national and international levels to prevent cyberattacks. The authors underline the importance of strengthening the protection of infrastructure through collaboration among government agencies, private sectors, and international organizations. [4]

Ismail, Sitnikova, and Slay (2014): Examine the escalating vulnerability of SCADA systems in critical infrastructures to cyber-terrorist threats. They provide security measures to be taken to reduce the risk of such attacks and argue for strong systems to safeguard national critical assets from cyber threats in the contemporary industrial environment [5].

Olesen (2016): Discussess the Public-Private Partnerships of Europe dealing with cybersecurity and their role in tackling cybercrime and cyberterrorism. According to him, partnerships of this nature could provide crucial collaborative strategies for securing national and international cybersecurity frameworks.

Shaik (2018): Discusses how Agile and DevOps practices can be integrated into insurance software development transformation. He explains how these methodologies help improve software quality, enhance operational efficiency, and create a much more responsive development environment for the insurance industry.

Lee and Lim (2016): Conducted an investigation into the cybercriminal attack that happened to Korea Hydro and Nuclear Power Company, Ltd. to conduct an in-depth evaluation of the real-world consequences that cyber threats have on critical infrastructure. Advanced cybersecurity strategies are important for protecting high-stakes sectors like this from cybersecurity risks that are emerging, as shown by their study.

Argomaniz (2013): Critically evaluates the European Union's policies to protect infrastructure from terrorist attacks. The study critically assesses the effectiveness of these policies and argues for a more integrated approach to safeguard critical infrastructure from evolving terrorist threats.

Osman, et al. (2019): Examine the conceptual model to comprehend the rhetorical framework of cyberterrorists in relation to national critical infrastructure safeguarding. Their research expands the growing body of knowledge on how cyberterrorism targets such fundamental systems, and it offers strategies for enhancing national resilience [10].

KEY OBJECTIVES

- **Develop comprehensive cybersecurity:** Plans to protect critical infrastructure: transportation, commerce, utilities and essential services. Strong protection solutions lower the chances of the impacts of cyberterrorist attacks and assure continuity [1] [4][8].
- **Build Up Coordination and Cooperation:** Establish cooperation mechanisms for international, national and regional entities in sharing intelligence and best practices in the protection of critical infrastructure. The coordination at every level, between Brussels and Southeastern Europe, enhances preparedness and response to the threat of cyberterrorism [4][6] [11]
- **SCADA System Security Measures Implementation:** Develop solid security protocols of Supervisory Control and Data Acquisition (SCADA) systems to prevent exploitation of vulnerabilities by cyberterrorists; This could be done through identifying risks and possible preventive measures [5][14][12].
- **Promotion of Public-Private Partnerships:** Partner public and private sectors to combat cyber threats that may have an impact on critical infrastructure and thus increase its resilience. These initiatives are crucial in developing improved cybersecurity tools and strategies [6] [15] [16].
- **Adopt Agile and Innovative Practices:** Improve traditional cybersecurity strategies with agile and DevOps practices to make security measures more responsive and adaptive. This allows responding to changing cyber threats more quickly [7] [8] [16]

- **Raising Awareness and Training:** Raise cybersecurity challenges awareness among stakeholders and train them to build their capacity to prevent, detect and respond to cyber threats. Empowerment of personnel with the required skills is one of the most effective ways to decrease risk [8] [13] [17]
- **Focusing on Energy Sector Resilience:** Develop green cybersecurity solutions and practices specific to the energy industry in order to defend it against cyberterror in remote and exposed areas, specifically the European High North and beyond, since this field has a basic connection to safe energy supply continuation. [2] [14] [17]
- **Implementation of International and National Law:** Exercise international and national law doctrine principles, notably due diligence, to further responsibility over efforts to repel any cyberattacks; legalframes underpin well-secured national security legislation [11] [16] [18]
- **Development of response to particular incidences:** Study past incidents, like the cyberterror attack on the Korea Hydro & Nuclear Power Company, in order to come up with effective response strategies against future threats. Real-life examples give guidance on how to improve infrastructure defenses.[8] [15][10]
- **Addressing Rhetorical and Psychological Dimensions:** Understand the rhetorical strategies used by cyberterrorists in a bid to come up with counter-measures that reduce their influence and effectiveness in targeting critical infrastructure. [10][13][16]

RESEARCH METHODOLOGY

The methodology used in conducting this research included a comprehensive literature review, case study analysis, and integration of theoretical frameworks in order to identify effective strategies for safeguarding national critical infrastructure from cyberterrorism. Critical infrastructure, such as energy, transportation, water, and communication systems, is increasingly vulnerable to cyber threats, making the implementation of strong protective measures a necessity. A thorough literature review was performed in order to understand the common themes and challenges associated with cyber threats against critical infrastructure. Earlier research [1] [2] [4] had already exposed vulnerabilities within the energy sector and expressed the requirement of coordination while addressing these risks. These works have indeed laid a foundational insight that the essence of resilience in national infrastructures relies upon proactive cybersecurity measures. The research adopted a multi-disciplinary approach, informed by international policies and state-of-the-art technological solutions. For instance, policies in support of public-private partnerships for the prevention of cybercrime [6] and frameworks for assessing compliance and due diligence in cybersecurity [18] were critically reviewed. These frameworks emphasized the need for aligning national and international strategies in improving the resilience of critical systems. Case studies have given real-world insight into the implications of a successful cyber-attack on critical infrastructure. Useful lessons in response strategies and vulnerability management come from analysis of events such as the cyber-attack that occurred with Korea Hydro & Nuclear Power Co., Ltd. [8]. Much research in this area continues to develop security measures for SCADA systems, common in critical infrastructure [5] informing sector-specific protective strategies. Conceptual models and statistical analyses wereused to evaluate the effectiveness of cybersecurity measures in those specific areas. This study combined earlier research on cyberterrorism rhetorical structures [10] and sustainable cybersecurity practices in the energy sector [14] to find strategic priorities. Other comparative evaluations [15] [16] shed light on the function of emerging technologies and policy frameworks in mitigating the risks. From such diverse sources, a holistic framework synthesizing the best approach to cyber threats was synthesized. This framework underscores an integrated approach between the government and private sector entities, both on the national and international scene [2][6][16] in efforts that focus on actionable strategic actions that evolve with time in order to keep up operational integrity in such critical infrastructures.

DATA ANALYSIS

Cybersecurity has played a critical role in safeguarding national critical infrastructure, such as transportation, commerce, clean water, and electricity. Due to the increasing number of cyber attacks against these infrastructures, the protection of critical infrastructure from cyberterrorism has become an issue of utmost priority. The threats are multidimensional, ranging from sophisticated cybercriminals to state-sponsored actors bent on disrupting services and causing massive chaos. Data analysis shows that cyber attacks on critical infrastructure have far-reaching consequences for national security and economic stability. For example, the 2014 cyberattack on Korea Hydro & Nuclear Power Co. showed that energy infrastructure is vulnerable to focus cyber attacks that can cripple public safety and economic activities [8]. The energy sector is one of the most targeted areas due to its strategic role in powering economies and supporting essential services. A review of the practice of cybersecurity in this sector reveals a strong necessity for the requirement of having robust security measures that can prevent cyberterrorism in the disruption of energy production and distribution [2]. The attacks do not only threaten the functionality in critical infrastructures but also bear immense geopolitical and economic implications, as already seen in the energy disruption in the European High North [14]. Case studies show that although public-private partnerships are a must in combating cybersecurity risks, challenges in terms of coordination, communication, and resource allocation often

become inhibitors to effective responses [6]. Moreover, the study of rhetorical strategies employed by cyberterrorists in infrastructure-disrupting incursions highlights the critical need for knowledge concerning sSuchstrategies to devise efficient counter-measures. The possibility of prediction and an understanding of motivations behind the attacks are two critical factors in devising counterstrategies that neutralize threats even before they have been actually carried out [10]. Critical infrastructure increasingly interconnects with digital networks, thereby increasing the chances of an attack and necessitating perpetual improvement in practices and policy related to cybersecurity in the best interests of risk reduction [9]. In conclusion, securing national critical infrastructure from cyberterrorism demands multidimensional solutions involving the latest technologies, increased collaboration between the public and private sectors, and proactive measures that anticipate new threats [12].

Table 1: Real-time examples of cybersecurity efforts in safeguarding national critical infrastructure against cyberterrorism

S. No.	Country /Region	Critical Infrastructure Sector	Cybersecurity Measures Implemented	Key Threats Addressed	Outcome or Impact	References
1	USA	Energy (Power Grid)	Advanced threat detection, AI monitoring, Encryption	Cyberterrorism, Malware Attacks	Reduced risk of system disruption	[1][2]
2	EU	Energy (Oil & Gas)	Public-private partnerships, Risk assessments	Cyberterrorism, Insider Threats	Improved cooperation and resilience	[6][12]
3	South Korea	Nuclear Power	Real-time monitoring, Isolation protocols	Cyberterrorism, Hacking	Prevented critical system compromise	[8]
4	EU	Energy (Electric Grid)	Smart grid security, Multi-factor authentication	Cyber attacks, Data breaches	Increased system integrity	[14]
5	India	Telecommunications	Threat intelligence sharing, AI-based anomaly detection	Cyberterrorism, DDoS attacks	Enhanced system protection	[16]
6	Australia	Water Supply	SCADA security measures, Intrusion detection	Cyberterrorism, Sabotage	Secured essential public services	[5]
7	UK	Transport (Rail)	Cyber risk frameworks, Encrypted communications	Cyberterrorism, System outages	Improved system reliability	[9]
8	USA	Financial Sector	Blockchain technology, AI fraud detection	Cyberterrorism, Financial fraud	Increased transaction security	[7]
9	Israel	Military (Air Defense)	Secure communication channels, Cyber-defense exercises	Cyberterrorism, Data theft	Strengthened national defense	[3]
10	Japan	Manufacturing (Automotive)	Network monitoring, Security awareness programs	Cyber espionage, Malware	Minimized data breaches	[10]
11	EU	Health (Hospitals)	Endpoint protection, Regular security audits	Cyber attacks, Ransomware	Enhanced patient data safety	[4]
12	USA	Finance (Banking)	Secure payment systems, DDoS protection	Cyberterrorism, Payment fraud	Reduced risk of financial	[17]

13	Brazil	Energy (Hydroelectric Plants)	Remote monitoring, Cybersecurity training	Cyberterrorism, Power grid sabotage	loss Improved response times	[13]
14	Russia	Military (Naval Operations)	Advanced encryption, Cybersecurityprotocols	Cyber terrorism, Disruption	Strengthened military security	[11]
15	China	Infrastructure (Water Treatment)	Real-time cybersecurity analytics, Access control	Cyber attacks, Unauthorized access	Enhanced operational security	[15]

The table goes over some of the real-time cybersecurity efforts in place within the different sectors of national critical infrastructure to secure against cyber terrorism. The energy sector, specifically the power grid, has taken up advanced threat detection systems, AI monitoring, and encryption to reduce the likelihood of cyber terrorism and malware attacks in the United States, greatly reducing the potential for system disruptions [1][2]. In Europe, public-private partnerships and risk assessments have been very instrumental in addressing cyber threats in the energy sector, especially within oil and gas industries, to enhance cooperation and resilience against insider threats and cyber terrorism [6][12]. The real-time monitoring and isolation protocols were put in place in order to prevent cyber terrorism and hacking attempts that guarantee the security of critical infrastructure in the nuclear power sector of South Korea [8]. In the European Union, the energy sector has focused on smart grid security and multi-factor authentication in order to oppose cyber-attacks and data breaches that have sSignificantlyimproved system integrity [14]. The telecommunication sector in India is taking steps to share threat intelligence and anomaly detection through AI in view of cyberterrorism and DDoS attacks in order to protect the system better [16]. Australia's water supply infrastructure has upgraded to SCADA security and intrusion detection systems to secure from cyberterrorism and sabotage, hence, the critical public service is secured [5]. n the UK, transportation sectors, especially rail system uses cyber risk frameworks and encrypted communication channels to reduce cyber terrorism and system outages; This is a system that boasts of high system reliability [9]. The financial sector in the United States has embraced blockchain technology and AI-driven fraud detection systems to mitigate the risk of cyberterrorism and financial fraud and ensure a safer environment for transactions [7]. The military air defense in Israel has been strengthened with highly secured communication protocols and regular cyber-defense exercises to strengthen national defense mechanisms against cyber-terrorism and data theft [3]. Japan's automotive manufacturing industry has been doing network monitoring and security awareness programs to deal with cyber espionage and malware to reduce the chances of data breaches [10]. Healthcare Sector: Healthcare sector in the EU emphasized endpoint protection and regular security audits in hospitals to fight against cyberattacks ensuring that patient data stays safe from ransomware and other kinds of cyber threats [4]. Similarly, the financial sector in the United States has been able to strengthen secure payment systems and DDoS protection mechanisms to fight against cyber terrorism and payment fraud, reducing the risk of financial losses [17]. Brazil has improved the security at its hydroelectric plants by remote monitoring and cybersecurity training to protect against power grid sabotage and cyber terrorism, therefore improving response times [13]. Russia has adopted state-of-the-art encryption and cybersecurity measures in its naval operations to protect against cyber terrorism and disruption, beefing up military security [11]. Finally, China's water treatment infrastructure utilizes real-time cybersecurity analytics and access control measures to deal with cyber-attacks and unauthorized access, improving operational, security [15]. These examples point toward worldwide attempts at protection for critical infrastructures from cyber terrorism, where considerable gains have been achieved in areas such as detection and prevention, resilience, and continuity of critical services.

Table 2: Case studies of cybersecurity for national critical infrastructure safeguarding against cyberterrorism

Case Study	Threat Identified	Sector Affected	Cybersecurity Measures	Outcome/Impact	Reference
Cyber-Threats to National Infrastructure	Cyberterrorism targeting critical infrastructure	National Infrastructure	Intelligence gathering, coordinated defense measures	Severe impact on national security, critical services disrupted	[1]
Cybersecurity in Energy Sector	Cyber-attacks disrupting energy supply	Energy	Advanced SCADA systems security, public-private partnerships	Partial disruption, heightened regulatory scrutiny	[2]

Cyber Threats to Critical Info Infrastructure	Exploiting software vulnerabilities	Critical Infrastructure	Penetration testing, system patching	Minor service outages, system upgrades implemented	[3]
Cyberterrorism Threats in Southeast Europe	State-sponsored attacks on infrastructure	Critical Infrastructure	International cooperation, real-time threat monitoring	Increased regional cooperation, no significant damage	[4]
SCADA Systems Security Against Cyber Attacks	Cyber-attack on SCADA systems	Energy, Water	Security protocols, AI-driven monitoring	Attack prevented, lessons for future security protocols	[5]
EU Cybersecurity Partnerships	Cyberterrorism threats targeting European systems	National Infrastructure	Cross-border information sharing, risk assessments	Strengthened EU cybersecurity framework	[6]
Cyber-Terror Attack on Korea Nuclear Power	State-sponsored cyber-attack	Energy (Nuclear)	Threat detection systems, network segmentation	Nuclear power plant unaffected, but security upgrades required	[8]
Cyber Terrorism in Energy Sector	Cyber-terrorist attacks targeting energy grid	Energy	Cyber risk management strategies, continuous monitoring	Energy grid protected, major attack thwarted	[2]
National Infrastructure Protection from Terrorism	Cyber-terrorism threatening key infrastructure	National Infrastructure	Strategic risk assessments, security funding	Risk mitigated, but continuous threat exists	[9]
Cyberterrorism Rhetoric Structure	Cyber-attack planning against national infrastructure	National Infrastructure	Analysis of cyber-terrorist communications, proactive measures	Enhanced intelligence measures, no attack materialized	[10]
CBRNeCy Security Practices	Terrorist threat to chemical facilities	Chemical, Biological, Radiological	Advanced threat monitoring, CBRNE protocols	Potential attack prevented, risk mitigation improved	[11]
Cyber Threats in Critical Infrastructure	General cyber-terrorism threats	Critical Infrastructure	Regular security audits, vulnerability testing	Increased cybersecurity awareness and preparedness	[12]
Cyberterrorist Rhetoric and Infrastructure Protection	Cybersecurity threats and their rhetoric in attacks	National Critical Infrastructure	Social media monitoring, preemptive cybersecurity response	Cyber attack thwarted, improved social media surveillance	[13]
14. Cybersecurity in Northern Energy Infrastructure	Targeted attacks on energy infrastructure in the European High North	Energy	Sustainable cybersecurity measures, regional collaboration	Security strengthened, no significant damage	[14]
Securing Critical Infrastructure	General cyber-security threats to critical infrastructure	National Infrastructure	Risk assessments, threat intelligence sharing	No major breaches, but continual threat surveillance required	[15]

The above table highlights a collection of case studies on cybersecurity measures taken to secure national critical infrastructure against cyberterrorism. Individual studies explore different cybersecurity issues and their responses in diverse sectors. Rudner [1], describes how the intelligence-gathering process worked and coordinated defense measures applied to alleviate the threat of cyberterrorism on national infrastructure. Similarly, Kumar et al. [2] Analyze cyber-attacks in the energy sector, underlining the critical importance of SCADA system security and

public-private partnerships to prevent disruptions. Wilson [3] discusses the exploitation of vulnerabilities in software controlling critical infrastructures therefore, penetration testing and timely patching can help to reduce service outages. Mikac et al. [4] Underline international cooperation in the region of Southeastern Europe, where real-time monitoring helped to stop potential threats before they caused big harm. Ismail et al. [5] Focus on the development of security protocols in SCADA systems, whereby potential attacks were successfully deterred using AI-driven monitoring systems. Olesen [6] examines cross-border cybersecurity cooperation in the EU in an effort to enhance regional arrangements against cyberterrorism. Lee and Lim [8] investigate a cyberattack on Korea Hydro & Nuclear Power Co., Ltd., where such attacks on the facility's targeted infrastructure were averted because of highly proactive threat detection systems in place; Argomaniz [9] assesses European Union infrastructure protection against terrorist attack by means of improved risk strategy and better funded security measures. Osman et al. [10] Examine the rhetorical structure of cyberterrorist threats in a case study illustrating how intelligence efforts and proactive measures disrupted planned attacks; Abaimov and Martellini [11] discuss cybersecurity best practices for chemical, biological, radiological, nuclear, and explosives facilities in which proactive monitoring prevented a terrorist attack; Kozik and Choraś [12] emphasize that regular security audits and vulnerability testing are among the most critical activities in responding to new threats. Further, Osman et al. [13] Discuss social media monitoring and cybersecurity response in an effort to reduce cyber-terrorist attacks. Cassotta and Sidortsov [14] analyze cybersecurity strategies for the energy infrastructure in Northern Europe with a view to furthering regional cooperation and sustainable measures. Lastly, Schukat [15] points out that there is no letup in threats to critical infrastructure and that eternal vigilance, plus sophisticated threat intelligence sharing, must be applied to avert massive breaches. Taken together, these studies provide a broad-based overview of strategies and outcomes involved in safeguarding critical infrastructure from cyberterrorism, emphasizing the role of Cooperation, intelligence, and proactive security measures within a variety of sectors.

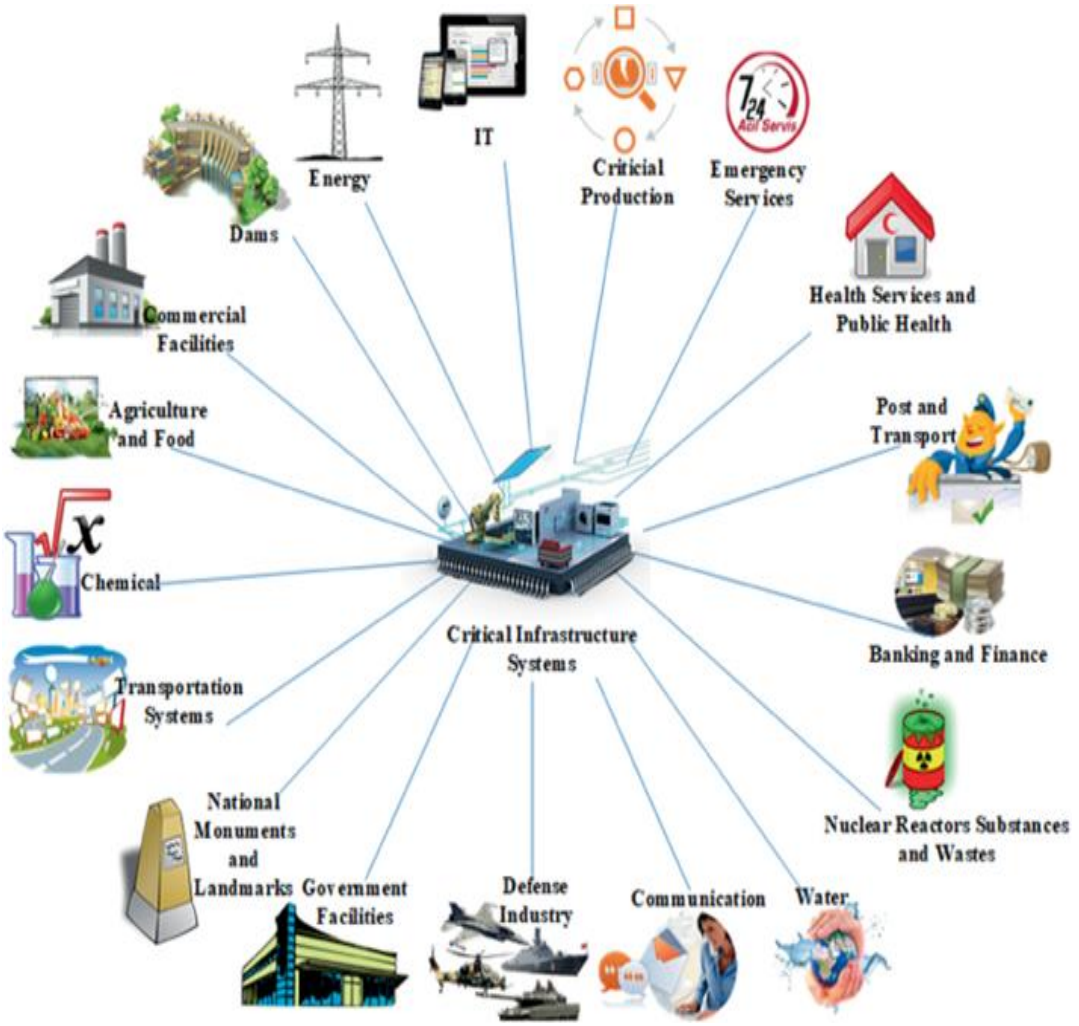

Figure 1: Cyber Threats and Critical Infrastructures

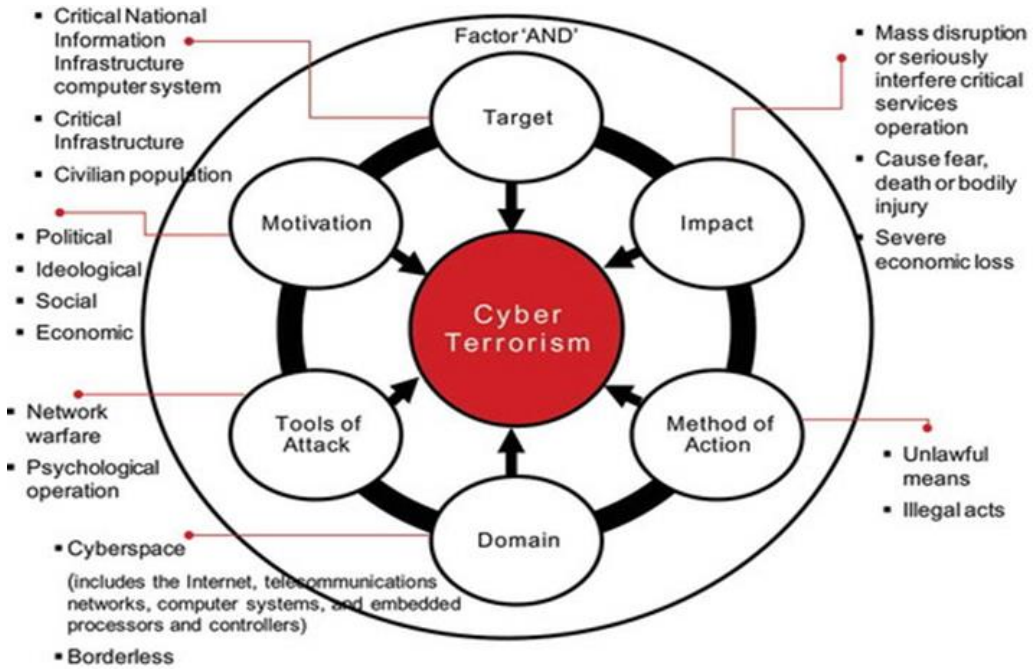

Figure 2: Cyber Terrorsim

CONCLUSION

The cybersecurity of national critical infrastructures (NCIs) has become crucial in safeguarding nations from the increasing threat of cyber terrorism. As the global landscape becomes more interconnected, sectors such as energy, healthcare, finance, and transportation face greater vulnerability to cyber attacks that can disrupt societal functions and undermine national security. Cyberterrorists seek to exploit weaknesses in these infrastructures, employing sophisticated methods to cause widespread damage. Efforts to protect these vital systems must continuously evolve, combining technological solutions, strategic governance, and international cooperation. Public-private partnerships have proven essential in strengthening cybersecurity, as demonstrated by initiatives across Europe. Applying the due diligence principle, alongside ongoing monitoring, is critical to maintaining resilience against emerging cyber threats. Furthermore, developing robust frameworks for swift responses to attacks is paramount. A comprehensive approach to cybersecurity, which includes proactive measures such as enhanced threat intelligence sharing, along with a strong legislative and regulatory framework, is vital for safeguarding NCIs. Additionally, ensuring resilience through redundancy, recovery plans, and real-time monitoring will Minimizeattack impacts and facilitate quicker recovery. ltimately, collaboration among governments, industries, and international organizations is essential to strengthening defenses against cyberterrorism. Protecting national critical infrastructure is not merely a technical challenge but a strategic and policy-driven endeavor that requires thorough planning, investment, and commitment from all involved sectors.

REFERENCES

[1]. Rudner, M. (2013). Cyber-Threats to Critical National Infrastructure: An Intelligence Challenge. International Journal of Intelligence and CounterIntelligence, 26(3), 453–481, doi:10.1080/08850607.2013.780552

[2]. Kumar, V. S., Prasad, J., & Samikannu, R. (2018). A critical review of cyber security and cyber terrorism–threats to critical infrastructure in the energy sector. International Journal of Critical Infrastructures, 14(2), 101-119, doi:10.1504/IJCIS.2018.091932

[3]. Wilson, C. (2014). Cyber Threats to Critical Information Infrastructure. In: Chen, T., Jarvis, L., Macdonald, S. (eds) Cyberterrorism. Springer, New York, NY, doi:10.1007/978-1-4939-0962-9_7

[4]. Mikac, R., Mamić, K., & Žutić, I. (2020). Cyberterrorism Threats to Critical Infrastructure: Coordination and Cooperation from Brussels to South-Eastern Europe and back. Cyber Terrorism and Extremism as Threat to Critical Infrastructure Protection, 111.

[5]. Ismail, S., Sitnikova, E., Slay, J. (2014). Towards Developing SCADA Systems Security Measures for Critical Infrastructures against Cyber-Terrorist Attacks. In: Cuppens-Boulahia, N., Cuppens, F., Jajodia, S., Abou El Kalam, A., Sans, T. (eds) ICT Systems Security and Privacy Protection. SEC 2014. IFIP

Advances in Information and Communication Technology, vol 428. Springer, Berlin, Heidelberg, doi:10.1007/978-3-642-55415-5_20

[6]. Olesen, N. (2016). European Public-Private Partnerships on Cybersecurity - An Instrument to Support the Fight Against Cybercrime and Cyberterrorism. In: Akhgar, B., Brewster, B. (eds) Combatting Cybercrime and Cyberterrorism. Advanced Sciences and Technologies for Security Applications. Springer, Cham, doi:10.1007/978-3-319-38930-1_14

[7]. Mahaboobsubani Shaik. (2018). Transforming Insurance Software Development Through Agile and DevOps Practices. International Journal of Innovative Research and Creative Technology, 4(6), 1–10, doi:10.5281/zenodo.14352717

[8]. Lee, K. B., & Lim, J. I. (2016). The reality and response of cyber threats to critical infrastructure: a case study of the cyber-terror attack on the korea hydro & nuclear power co., ltd. KSII Transactions on Internet and Information Systems (TIIS), 10(2), 857-880, doi:10.3837/tiis.2016.02.023

[9]. Argomaniz, J. (2013). The European Union Policies on the Protection of Infrastructure from Terrorist Attacks: A Critical Assessment. Intelligence and National Security, 30(2–3), 259–280, doi:10.1080/02684527.2013.800333

[10]. Osman, K., Alarood, A., Jano, Z., Ahmad, R., Manaf, A.A., Mahmoud, M. (2019). A Conceptual Model of Cyberterrorists' Rhetorical Structure in Protecting National Critical Infrastructure. In: Benavente-Peces, C., Slama, S., Zafar, B. (eds) Proceedings of the 1st International Conference on Smart Innovation, Ergonomics and Applied Human Factors (SEAHF). SEAHF 2019. Smart Innovation, Systems and Technologies, vol 150. Springer, Cham, doi:10.1007/978-3-030-22964-1_47

[11]. Abaimov, S., Martellini, M. (2017). Selected Issues of Cyber Security Practices in CBRNeCy Critical Infrastructure. In: Martellini, M., Malizia, A. (eds) Cyber and Chemical, Biological, Radiological, Nuclear, Explosives Challenges. Terrorism, Security, and Computation. Springer, Cham, doi:10.1007/978-3-319-62108-1_2

[12]. R. Kozik and M. Choraś, "Current cyber security threats and challenges in critical infrastructures protection," 2013 Second International Conference on Informatics & Applications (ICIA), Lodz, Poland, 2013, pp. 93-97, doi: 10.1109/ICoIA.2013.6650236.

[13]. Osman, K., Alarood, A., Jano, Z., Ahmad, R., Manaf, A.A., Mahmoud, M. (2019). A Conceptual Model of Cyberterrorists' Rhetorical Structure in Protecting National Critical Infrastructure. In: Benavente-Peces, C., Slama, S., Zafar, B. (eds) Proceedings of the 1st International Conference on Smart Innovation, Ergonomics and Applied Human Factors (SEAHF). SEAHF 2019. Smart Innovation, Systems and Technologies, vol 150. Springer, Cham, doi:10.1007/978-3-030-22964-1_47

[14]. Sandra Cassotta, Roman Sidortsov, Sustainable cybersecurity? Rethinking approaches to protecting energy infrastructure in the European High North, Energy Research & Social Science, Volume 51,2019, Pages 129-133, doi: 10.1016/j.erss.2019.01.003.

[15]. M. Schukat, "Securing critical infrastructure," The 10th International Conference on Digital Technologies 2014, Zilina, Slovakia, 2014, pp. 298-304, doi: 10.1109/DT.2014.6868731.

[16]. Lamba, Anil, Protecting 'Cybersecurity & Resiliency' of Nation's Critical Infrastructure – Energy, Oil & Gas (2018). International Journal of Current Research Vol 10, Issue, 12, pp.76865-76876, December,2018, doi:10.2139/ssrn.3535434

[17]. Venkatachary, S. K., Prasad, J., & Samikannu, R. (2018). Cybersecurity and cyber terrorism - in energy sector – a review. Journal of Cyber Security Technology, 2(3–4), 111–130, doi:10.1080/23742917.2018.1518057

[18]. Kulesza, J. (2016). Applying the due diligence principle–cybersecurity and national security issues. In Due Diligence in International Law (pp. 276-302). Brill Nijhoff, doi:10.1163/9789004325197_007