TECHNICAL UNIVERSITY OF CLUJ-NAPOCA

ACTA TECHNICA NAPOCENSIS

Series: Applied Mathematics, Mechanics, and Engineering
Vol. 68, Issue IV, November, 2025

THE OPERATIONAL AND TECHNOLOGICAL SAFETY AND SECURITY OF THE EUROPEAN CRITICAL INFRASTRUCTURE IN THE LIGHT OF ENERGY CRISES

Ricardo P. ARCINIEGA-ROCHA, Vanessa C. ERAZO-CHAMORRO, Gyula SZABÓ

Abstract: *This study explores the operational and technological safety and security of European Critical Infrastructure (ECI) amid escalating energy crises. With the rise of Industry 4.0 and digital technologies—such as IoT, AI, and 5G—CI systems have become increasingly interconnected and vulnerable to cyber threats, natural disasters, and geopolitical tensions. The paper highlights the importance of Critical Infrastructure Protection (CIP) through multidisciplinary approaches, risk management, and public-private collaboration. Using text analysis and real-world case studies, the authors examine the impact of energy shortages on industrial productivity, economic stability, and societal well-being. The research underscores the urgent need for robust, adaptive strategies to safeguard CI and ensure resilience in the face of growing global energy demands and digital dependencies.*
Key words: *Critical Infrastructure, Energy, Operational technologies, Safety.*

1. INTRODUCTION

Critical infrastructure protection (CIP) has emerged as a new area of European integration. With the advent of the digital age in the mid-20th century and the introduction of Industry 4.0, traditional industries gave way to an economy based on the Internet and information and communication technologies (ICTs). Big data, cloud computing, the Internet of Things (IoT), mobile devices, artificial intelligence, 5G networks and other ICTs are being used by many people around the world, not just businesses.

There is little doubt that the application of digital technology in various industries has increased output while reducing prices. One of the obvious implications of the development of Industry 4.0 is digital culture. On the other hand, the risks associated with digital culture, including ICT, could jeopardize the operational and technological safety and security of Europe's critical infrastructure. The operational and technological safety and security of Europe's critical infrastructure is one of the most pressing issues. In this exploratory study, we used text analysis as a research tool to understand the operational and technological security of Europe's critical infrastructure and to assess the problems using real cases.

Critical infrastructure protection (CIP) has emerged as a new area of European integration. Traditional industries gave a place to an economy based enormously on Internet and Information and Communication Technologies (ICT) with the entrance of the digital era in the mid-twentieth century and the introduction of Industry 4.0. Big data, cloud computing, the Internet of Things (IoT), mobile devices, artificial intelligence, 5G networks, and other ICTs are being used by a growing number of people globally, not only enterprises [1]–[4].

Critical infrastructure (CI) of national importance in countries supposes the CI which in a possible suspension or abolition of its operations would have serious consequences for national security, the economy, and other critical social functions, as well as people's health, safety, protection, and well-being.

The EU institutions and agencies are now involved in everything from pandemic

Received: 10.09.25; **Similarities**: 20.10.25: **Reviewed**: 10.09./ 10.09.25: **Accepted**:18.11.25.

preparation to food safety, disaster response, and counterterrorism initiatives. These initiatives herald the emergence of a "European protection policy space" and a qualitatively new type of cooperation in the EU [5]. The ECI is regulated by the Regulation on European Critical Infrastructure (2011), to establish the needs and the definition of ECI fields and characteristics designated location on each country member [6].

The volume of personal data collected and the flow of information about users is increasing in tandem with the increasing digitalization of business and the rapid development of information and communications technology. This increases the likelihood of abuse and violation of privacy rights. As a result, the EU adopted the General Data Protection Regulation - GDPR (2016), which aims to harmonize and raise the level of personal data protection in various EU sectors, including the maritime sector.

Cyber security attacks on Operational technologies (OTs) can cause explosions, collisions, and blackouts. This necessitates novel risk management practices that also address security and safety concerns [7]–[11]. Automation and control systems, such as Supervisory Control and Data Acquisition (SCADA), are referred to as monitor and control systems power, pipelines, water distribution, sewage systems, and production control are all, this relation connected to Operational Technology (OT).

Natural disasters and extreme weather put energy infrastructures, like distribution and production networks, at risk. These infrastructures are crucial for essential societal functions like people's health, safety, security, economic, and social well-being, which is why they are referred to as critical infrastructures (a catch-all term that encompasses the transportation, technology for communication and information (ICT), water, and emergency sectors, among others) (Directive 2008/114/EC). Natural disasters and extreme weather put energy infrastructures, like distribution and production networks, at risk. Energy Critical Infrastructure (ECI) systems have already failed due to natural disasters or unintentional malfunctions, with dire ramifications for the economy and society [12]–[14].

A "system of systems," modern infrastructures have multiple dependencies, interactions, and interconnections. Damage to one infrastructure system can therefore lead to failures and have a domino effect on all other linked and dependent infrastructures, so impacting the community and economy as a whole [9], [15].

Critical Energy Infrastructure (CEI) is a prime target for various types of attacks. However, CEI is vulnerable not only to terrorist attacks, but also to state attacks such as extensive energy "denial" operations during countries' wars [16].

In the context of all mentioned above the operational and technological safety and security of the ECI considering energy crises presents a field with a deep gap to define the protocols and operational procedures to avoid the biased management of the CEI. In this sense the rest of the document is organized as follows: Section 2 Related Works shows previous studies in this context. Section 3 Methodology presents the steps for data collection and information processing for analysis. Section 4 Results presents the outcomes of the research. Finally, Section 5 Conclusions presents a discussion of the results and research conclusions.

2. RELATED WORKS

In 2004 Farrell developed research on Energy Infrastructure and Security, how such a connection differs from conventional energy security aspects, and what that may necessarily imply for private and policy decisions [17].

During 2015 Mehravari presents the cybersecurity capabilities of the energy-critical infrastructure evaluation using C2M2 model to demonstrate how these models have been successfully implemented by an increasing number of entities, and plans for their ongoing stewardship, evolution, and application to other types of organizations [18].

In 2017 Mikellidou presents a review about Energy critical infrastructures at risk from climate change, identifying risk assessment, interdependence with other sectors, and adaptation/resilience options are all important aspects of CI protection [12].

3. METHOD DESCRIPTION

In the modern era, there is a scarcity of talent to implement digital control. As a result, as a new industry 4.0 niche emerges, digital Energy critical infrastructures education plays an important role in the spread of digital control.

To define the study and investigation gap, we performed this exploratory research using different research methods: content analysis and reviewing massive secondary research to better understand the situation of Energy critical infrastructures in Europe [12].

The literature and data are from reputed journals, the official website of the European Union, and so on. We also considered Roger's Diffusion of Innovation Theory (DOI), to gain a complete overview of "how" to adapt and use digital technologies to protect Energy critical infrastructures [13]. The key to getting energy-critical infrastructure protection actors to adopt digital technologies is to change their perception of them [14].

4. RESULTS

Considering energy crises, ECI considers multidisciplinary approaches by incorporating technological, environmental, and social aspects of energy structures, as well as close collaboration among multiple fields of research, such as energy planning, transportation infrastructure, and regulatory issues.

4.1. Types of energy crisis

Two main energy sources are identified as renewable and nonrenewable energy sources can be used; however, nonrenewable sources such as natural gas, fossil fuels, oil, and coal are not infinite and will be depleted; on the other hand, renewable energy sources do not diminish [19].

Since energy is one of our human civilization’s most basic needs, its supply should be reliable and plentiful. In this sense, electrical energy become the most usable energy source, due to its primary role in development the of industries in countries [20]. China and India's emerging economies are driving much of the world's rising energy demand. These two countries already account for half of global demand growth, and by 2030, their consumption is expected to more than double [21].

One of the main causes of the crisis is the continuous rise in the population, which is identified by international environmental organizations and international law providers [22]. Fig. 1 shows the identified causes of the energy crisis in the world.

The energy crisis is identified in terms of the relation between capital and product, besides the relation between work capacity and energy, due to the energy providing the necessary resources to convert the work activity into the product and directly this product provides a future capital for economies. In this field, the possible causes with the capacity to produce an energy failure have an enormous interest for countries [23], [24].

The energy crisis affects not only people's daily lives but also countries' development and progress. Because of a lack of energy in the form of electricity and natural gas, the industry is declining, and the transportation and domestic sectors are also suffering because of this crisis. To operate continuously, all major sectors, including industry, transportation, domestic, and power generation, require increasing amounts of energy [25].

Fig. 1. Causes of energy crises [20].

4.2. Energy crisis and workplaces

Renewable energy resources have grown in popularity due to their perpetual renewability, modularity, local availability, and environmental friendliness. The increase in

domestic and private consumption is due to increased economic well-being and technological innovations that introduce more energy-using applications to domestic and private users. The decrease in industrial energy consumption is due to technological advancements that provide highly efficient devices with high safety and reliability [26]–[28].

"Workers" and "employees" in the industry environment correspond to the "stable salaried working class," In terms of the economy this class needs to convert their forces into a product and energy became a main resource to be applied for them in their task. Besides the task, there are other characteristics like transportation for workers and products [28]–[30].

CI in the workplace can be significant and wide-ranging going from the disruption or cessation of essential services or processes. This can result in downtime, reduced productivity, missed deadlines, financial losses, and going through risks to employee safety and well-being. For example, power outages can lead to inadequate lighting, compromised security systems, or the loss of essential life support systems. Equipment failures or physical security incidents. Besides, Cybersecurity incidents targeting CI can result in data breaches, compromising sensitive information about the organization, its employees, or customers [31].

4.3. Critical Infrastructure

The term "critical infrastructure" (CI) refers to structural systems that, if suspended or eliminated, would have serious consequences for national security, the economy, and other critical social functions, as well as people's health, safety, protection, and well-being, it could be in both public and private, are among the "critical sectors" that may be affected and thus have a negative impact on the orderly operation of societal functions [32]. Fig. 2 presents the most important sectors in CI field.

Terrorists around the world have targeted the CI, resulting in uncontrollable fear, distrust, and other feelings that have a heavy impact on societal life and a wide range of side effects, including economic and psychological ones [33]. In this sense, CI protection became an important policy to be included in all states and countries around the world.

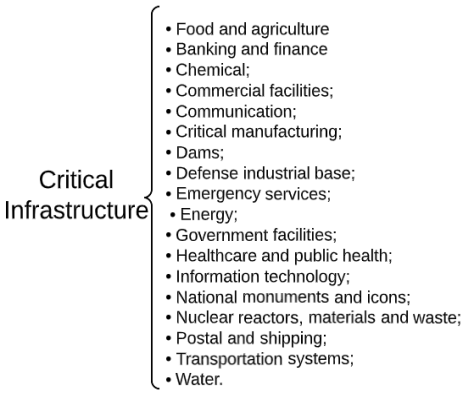

Fig. 2. Critical Infrastructure.

4.4. Critical Infrastructure Protection

Experiences with CIP in different countries have an important factor that all governments will never underestimate in the future: communication will be the main factor to control and protect all network systems for CI. The policymakers fighting for CIP have deeply understood the need to create public opinion around global security issues, with the particular goal of increasing citizens' preparation to face even now the deepest nightmare which may come true [34], [35].

CIP entails strengthening critical infrastructure frameworks to survive and recover from a variety of threats, such as natural disasters, accidents, cyber-attacks, and terrorist activities. Risk management is critical in identifying vulnerabilities, assessing potential threats, and implementing risk mitigation measures. This includes creating solid contingency plans, redundancy mechanisms, and backup systems to ensure operational continuity [36], [37]. Close collaboration and coordination between public and private entities is required for effective CIP.

It is critical for stakeholders to share information, intelligence, and best practices to improve situational awareness, early warning systems, and response capabilities.

Table 1

Energy Crises and Critical Infrastructure Protection.

Section	Key Concept	Details

Types of Energy Crisis	Energy Sources	Nonrenewable: Finite resources (e.g., natural gas, fossil fuels, oil, coal) that will be depleted.
		Renewable: Inexhaustible sources (e.g., solar, wind) that do not diminish.
	Energy Demand	Rising global energy demand, particularly driven by emerging economies like China and India.
		By 2030, consumption in these countries is expected to more than double.
	Causes of Energy Crisis	- Population growth.
		The critical relationship between capital, product, work capacity, and energy.
		Energy is essential for economic stability and development.
	Impact of Energy Crisis	- Affects daily life, industrial growth, transportation, and domestic sectors.
		- Insufficient energy supply leads to a decline in these sectors, impacting overall progress and development.
Energy Crisis and Workplaces	Renewable Energy Growth	Renewable energy is gaining popularity due to renewability, environmental benefits, and local availability.
		Economic well-being and technological advancements increase domestic energy consumption.
		Industrial energy use decreases with more efficient and reliable technologies.
	Workplace Impact	Workers in the industry rely heavily on energy for productivity.
		Energy crisis can lead to disruption of essential services, reduced productivity, financial losses, and safety risks.
		Critical Infrastructure (CI) failures (e.g., power outages, cybersecurity incidents) have far-reaching consequences.
Critical Infrastructure (CI)	Definition and Importance	CI includes systems critical to national security, the economy, and public health/safety.
		Affects both public and private sectors, impacting societal functions.
	Threats to CI	CI is a target for terrorism, leading to severe economic, psychological, and societal disruptions.
Critical Infrastructure Protection (CIP)	Protection Strategies	CIP involves strengthening CI to withstand threats like natural disasters, cyber-attacks, and terrorism.
		Risk management, contingency plans, redundancy mechanisms, and backup systems are vital.
	Collaboration and Coordination	Effective CIP requires collaboration between public and private entities, including governments, law enforcement, and infrastructure operators.
		Information sharing and partnerships are essential for comprehensive protection and improving response capabilities.

Partnerships between the public and private sectors also make it easier to allocate the resources, expertise, and technological advancements required for comprehensive infrastructure protection [38]. Table 1 shows the different aspects of energy crises, their impact on economies and jobs, and the importance of CIP.

5. CONCLUSIONS

The energy crisis is identified in terms of the relation between capital and product, besides the relation between work capacity and energy, due to the energy providing the necessary resources to convert the work activity into the product and this product is converted into capital for economies. The energy crisis affects not only people's daily lives but also countries' development and progress. Since energy is one of our human civilization's most basic needs, its supply should be reliable and plentiful. China and India's emerging economies are driving much of the world's rising energy demand. Because of a lack of energy in the form of electricity and natural gas, the industry is declining, and the transportation and domestic sectors are also suffering as a result of this crisis [19], [23].

The increase in domestic and private consumption is due to increased economic well-being and technological innovations that introduce more energy-using applications to domestic and private users. Besides the task, there are other characteristics like transportation for workers and products involved in the use of CI as a beneficiary.

The protection of critical infrastructure (CIP) has become a crucial aspect of European integration due to the increasing reliance on Internet and Information and Communication Technologies (ICT). With the rise of Industry 4.0 and the digital era, traditional industries have given way to an economy heavily based on ICT [39]. The use of big data, cloud computing, IoT, artificial intelligence, and 5G networks has become widespread, necessitating the establishment of robust measures to safeguard critical infrastructure.

The interdependencies and vulnerabilities of critical infrastructure systems pose significant challenges for their protection and management. Modern infrastructures are highly

interconnected and interdependent, which means that damage to one system can have cascading effects on others, impacting the entire community and economy. Furthermore, critical energy infrastructure (CEI) is not only vulnerable to terrorist attacks but also state attacks during times of conflict.

There is a pressing need to address the operational and technological safety and security of European CI to mitigate the risks associated with energy crises and potential malicious activities [40], [41].

The protection of critical infrastructure is a multifaceted effort that combines technical, operational, policy, and regulatory safeguards to protect critical systems from physical, cyber, and other threats. Societies can better withstand and recover from potential disruptions by prioritizing critical infrastructure protection and resilience, ensuring the safety, security, and operation of vital services and systems [4], [42].

Table 2 provides an overview of the energy crisis and critical infrastructure, analyzing the relationships between energy sources, demand, and their broader implications. Global energy demand is surging, particularly in rapidly developing economies.

This rising demand, coupled with population growth and the critical interplay between capital, productivity, and energy, underscores the causes of the energy crisis.

The essential connection between energy crises, their impact on the economy and the need for strong infrastructure protection, especially in Europe.

Energy is not only necessary for everyday activities, but also for the development of a country, as it transforms labor into products and drives economic progress.

A lack of energy can lead to industrial decline and disruptions in transport and housing, especially in rapidly developing countries. This is especially true as global demand for energy increases.

The growth of technology and economic prosperity is driving greater energy consumption in residential and commercial environments.

Table 2

CIP key points.

Topic	Key Points	Details
Energy Crisis and Economic Impact	Relation Between Capital, Product, Work Capacity, and Energy	- Energy is essential to convert work into products, which are then converted into capital for economies.
		- Energy crisis affects not only daily lives but also national development and economic progress.
	Global Energy Demand	- Rising energy demand driven by emerging economies like China and India.
		- Lack of energy in forms like electricity and natural gas leads to industrial decline and impacts transportation and domestic sectors.
Consumption Patterns	Increase in Domestic and Private Consumption	- Driven by economic well-being and technological innovations, leading to more energy-using applications in homes and private sectors.
		- Other factors include transportation needs for workers and products.
Critical Infrastructure (CI)	Importance of CIP in Europe	- CIP has become crucial in Europe due to reliance on Internet and ICT with the rise of Industry 4.0 and the digital era.
		- Widespread use of technologies like big data, cloud computing, IoT, AI, and 5G networks demands robust measures to safeguard critical infrastructure.
	Interdependencies and Vulnerabilities	- Modern infrastructures are highly interconnected, so damage to one system can cause cascading effects on others, affecting communities and economies.
		- Critical Energy Infrastructure (CEI) is vulnerable to terrorist and state attacks, especially during conflicts.
CIP Strategies	Protection and Resilience Measures	- CIP requires a combination of technical, operational, policy, and regulatory safeguards to protect systems from physical, cyber, and other threats.
		- Prioritizing CIP helps societies withstand and recover from disruptions, ensuring the safety and operation of vital services and systems.

Due to the increased reliance on digital technologies such as big data, IoT, AI and 5G networks, all of which require robust security measures, the importance of critical infrastructure protection (CIP) has grown [43], [44]. CIP strategies use a combination of operational, policy, technical and regulatory approaches to protect against and remediate

various threats. This ensures that critical services and systems are resilient enough to withstand and recover from potential disruptions.

Every day, people and businesses alike may suffer greatly when essential infrastructures, such as water systems, electricity grids, transportation networks, or digital communication platforms, are targeted. People may experience an abrupt loss of access to clean water, energy, healthcare, or even the internet, which can make daily life hazardous in addition to being challenging. Imagine transportation infrastructure malfunctioning, hospitals without electricity, or families without winter heating for their homes.

These attacks have the potential to disrupt business operations, postpone output, reveal confidential information, and endanger both assets and personnel. In the modern digital world, when everything is interconnected—whether via cloud computing, artificial intelligence, or the internet—an attack on one component of the system might lead to extensive failures in other areas. Entire businesses and communities may become paralyzed by these domino effects. Small interruptions can easily turn into large crises due to the world's growing energy consumption, population expansion, and the pressures of climate change. Protecting these systems is therefore no longer merely a technical problem; rather, it is a social duty that impacts everyone. Our everyday lives cannot function safely and successfully without effective cybersecurity, disaster preparedness, and tight collaboration between businesses and governments.

6. ACKNOWLEDGMENTS

This work was developed under co-participating Higher Technological Institute 17 July 2024.

7. REFERENCES

[1] Drăghici, A., Szabo, G., Gajšek, B., Mrugalska, B., Dovramadjiev, T., Zunjic, A., *Ergonomics and human factors in the Cyber Age. The case of Ergonomics and Human Factors Regional Educational CEEPUS Network*, Scientific Bulletin of the Politehnica University of Timişoara Transactions on Engineering and Management, vol. 8, no. 1–2, pp. 72–86, Apr. 2022, doi: 10.59168/RBWI1746.

[2] C. Pursiainen, “The Challenges for European Critical Infrastructure Protection,” *http://dx.doi.org/10.1080/07036330903199846*, vol. 31, no. 6, pp. 721–739, 2009, doi: 10.1080/07036330903199846.

[3] J. F. Rosero-Garcia, E. A. Llanes-Cedeño, R. P. Arciniega-Rocha, and J. López-Villada, “Analysis of Prediction and Clustering of Electricity Consumption in the Province of Imbabura-Ecuador for the Planning of Energy Resources,” *Lecture Notes in Networks and Systems*, vol. 284, pp. 1073–1084, 2021, doi: 10.1007/978-3-030-80126-7_75.

[4] E. Antonio *et al.*, “Analysis and Study of Energy Efficiency in the Electric System of the Millennium Education Schools "SUMAK YACHANA WASI of Imbabura Province in Ecuador,” *International Journal of Advanced Science and Technology*, vol. 29, no. 7, pp. 14040–14051, 2020, Accessed: Jan. 26, 2022. [Online]. Available: https://www.researchgate.net/publication/343375837.

[5] A. Boin, M. Ekengren, and M. Rhinard, “Protecting the Union: Analysing an Emerging Policy Space,” *https://doi.org/10.1080/07036330600979573*, vol. 28, no. 5, pp. 405–421, 2006, doi: 10.1080/07036330600979573.

[6] A. Androjna and E. Twrdy, “European Adriatic Sea-Way (EA Sea-Way) View project EA SEAWAY-European Adriatic Sea-Way View project CYBER THREATS TO MARITIME CRITICAL INFRASTRUCTURE,” Accessed: May 15, 2023. [Online]. Available: https://www.researchgate.net/publication/349502224.

[7] O. Michalec, S. Milyaeva, and A. Rashid, “When the future meets the past: Can safety and cyber security coexist in modern critical infrastructures?,” doi: 10.1177/20539517221108369.

[8] R.P. Arciniega-Rocha, V.C. Erazo-Chamorro, and G. Szabo, "The Prevention of Industrial Manual Tool Accidents Considering Occupational Health and Safety," *Safety*, vol. 9, no. 3, p. 51, Jul. 2023, doi: 10.3390/safety9030051.

[9] P.D. Rosero-Montalvo, V.F. López-Batista, R. Arciniega-Rocha, and D.H. Peluffo-Ordóñez, "Air Pollution Monitoring Using WSN Nodes with Machine Learning Techniques: A Case Study," *Logic Journal of the IGPL*, vol. 30, no. 4, pp. 599–610, Jul. 2022, doi: 10.1093/JIGPAL/JZAB005.

[10] P. Leisztner, "Occupational health and safety representatives and mediation," *Proceedings of FIKUSZ Symposium for Young Researchers*, 2022. https://www.proquest.com/conference-papers-proceedings/occupational-health-safety-representatives/docview/2769625528/se-2 (accessed Dec. 23, 2023).

[11] F. Faragó and G. Szabó, "Qualitative Assessment of the Occupational Health and Safety Knowledge Management Practices of Hungarian Companies," in *Lecture Notes in Networks and Systems*, 2023, vol. 701 LNNS, pp. 105–112, doi: 10.1007/978-3-031-33986-8_12.

[12] C. Varianou Mikellidou, L. M. Shakou, G. Boustras, and C. Dimopoulos, "Energy critical infrastructures at risk from climate change: A state of the art review," *Safety Science*, vol. 110, pp. 110–120, Dec. 2018, doi: 10.1016/J.SSCI.2017.12.022.

[13] K. Alutaibi, A. Alsubaie, and J. Martí, "A fire management decision support systems to minimise economic losses: A case study in a petrochemical complex," *International Journal of Critical Infrastructures*, vol. 14, no. 2, pp. 120–139, 2018, doi: 10.1504/IJCIS.2018.091933.

[14] 4 Hó, B. Sándor, and R. Nagy, "Védelem Tudomány-VI. Évfolyam, 2. Szám, 2021, Description and Investigation of it Systems Used in Disaster Management."

[15] V. S. Kumar, J. Prasad, and R. Samikannu, "A critical review of cyber security and cyber terrorism – threats to critical infrastructure in the energy sector," *International Journal of Critical Infrastructures*, vol. 14, no. 2, pp. 101–119, 2018, doi: 10.1504/IJCIS.2018.091932.

[16] I. Onyeji, M. Bazilian, and C. Bronk, "Cyber Security and Critical Energy Infrastructure," *The Electricity Journal*, vol. 27, no. 2, pp. 52–60, Mar. 2014, doi: 10.1016/J.TEJ.2014.01.011.

[17] A. E. Farrell, H. Zerriffi, and H. Dowlatabadi, "Energy infrastructure and security," *https://doi.org/10.1146/annurev.energy.29.062403.102238*, vol. 29, pp. 421–469, Oct. 2004, doi: 10.1146/ANNUREV.ENERGY.29.062403.102238.

[18] P. D. Curtis and N. Mehravari, "Evaluating and improving cybersecurity capabilities of the energy critical infrastructure," *2015 IEEE International Symposium on Technologies for Homeland Security, HST 2015*, Aug. 2015, doi: 10.1109/THS.2015.7225323.

[19] M. S. Javed *et al.*, "The energy crisis in Pakistan: A possible solution via biomass-based waste," *Journal of Renewable and Sustainable Energy*, vol. 8, no. 4, Jul. 2016, doi: 10.1063/1.4959974/840998.

[20] R. Poudyal, P. Loskot, R. Nepal, R. Parajuli, and S. K. Khadka, "Mitigating the current energy crisis in Nepal with renewable energy sources," *Renewable and Sustainable Energy Reviews*, vol. 116, p. 109388, Dec. 2019, doi: 10.1016/J.RSER.2019.109388.

[21] P. IEA and P. OECD, "World energy outlook 2008," 2008, doi: 10.3/JQUERY-UI.JS.

[22] S. Thomas, "Energy Efficiency Market Report - Capturing the Multiple Benefits of Energy Efficiency." International Association for Energy Economics, 2015, Accessed: May 30, 2023. [Online]. Available at: www.iaee.org/proceedings/article/13000.

[23] G. Caffentzis, "The Work/Energy Crisis and the Apocalypse."

[24] R. Nagy, "Konferenciakiadvány," pp. 73–86, Accessed: May 31, 2023. [Online]. Available: https://bgk.uni-obuda.hu/wp-content/uploads/2023/03/Szilvay-Kornel-Tuzvedelmi-Konferenciakiadvany-2023-PDF.pdf.

[25] A. Silvast, R. Kongsager, T. K. Lehtonen,

M. Lundgren, and M. Virtanen, “Critical infrastructure vulnerability: a research note on adaptation to climate change in the Nordic countries,” *https://doi.org/10.1080/00167223.2020.1851609*, vol. 121, no. 1, pp. 79–90, 2021, doi: 10.1080/00167223.2020.1851609.

[26] J. R. Murray, M. J. Minor, N. M. Bradburn, R. F. Cotterman, M. Frankel, and A. E. Pisarski, “Evolution of public response to the energy crisis,” *Science*, vol. 184, no. 4134, pp. 257–263, Apr. 1974, doi: 10.1126/SCIENCE.184.4134.257/ASSET/9DF8F7C6-0ECE-475C-83AC-67CAB33764AA/ASSETS/SCIENCE.184.4134.257.FP.PNG.

[27] V. C. Erazo-Chamorro, R. P. Arciniega-Rocha, and G. Szabo, “Safety Workplace: From of Point of View of Ergonomics and Occupational Biomechanics,” *Acta Technica Napocensis - Series: Applied Mathematics, Mechanics, And Engineering*, vol. 65, no. 3S, Jan. 2023, Accessed: Mar. 16, 2023. [Online]. Available: https://atna-mam.utcluj.ro/index.php/Acta/article/view/1949.

[28] V. C. Erazo-Chamorro, R. P. Arciniega-Rocha, N. Rudolf, B. Tibor, and S. Gyula, “Safety Workplace: The Prevention of Industrial Security Risk Factors,” *Applied Sciences*, vol. 12, no. 21, p. 10726, Oct. 2022, doi: 10.3390/app122110726.

[29] E. Krausmann, S. Girgin, and A. Necci, “Natural hazard impacts on industry and critical infrastructure: Natech risk drivers and risk management performance indicators,” *International Journal of Disaster Risk Reduction*, vol. 40, p. 101163, Nov. 2019, doi: 10.1016/J.IJDRR.2019.101163.

[30] V. C. Erazo-Chamorro, R. P. Arciniega-Rocha, and G. Szabo, “Healthy and safe workplace definition: a friendly boundary for a complex issue,” in *Mérnöki Szimpózium a Bánkin Előadásai : Proceedings of the Engineering Symposium at Bánki (ESB2021)*, 1st ed., vol. 1, Horváth Richárd, Ed. Budapest: Óbudai Egyetem, 2022, pp. 51–56.

[31] M. Curcuruto, S. M. Conchie, and M. A. Griffin, “Safety citizenship behavior (SCB) in the workplace: A stable construct? Analysis of psychometric invariance across four European countries,” *Accident Analysis & Prevention*, vol. 129, pp. 190–201, Aug. 2019, doi: 10.1016/J.AAP.2019.05.023.

[32] A. Lazari, “European critical infrastructure protection,” *European Critical Infrastructure Protection*, pp. 1–154, May 2014, doi: 10.1007/978-3-319-07497-9/COVER.

[33] M. Lindström, “The European programme for critical infrastructure protection,” in *Crisis Management in the European Union: Cooperation in the Face of Emergencies*, Springer Berlin Heidelberg, 2009, pp. 37–59.

[34] B. R. K Mantha *et al.*, “Construction cybersecurity and critical infrastructure protection: New horizons for Construction 4.0,” *Journal of Information Technology in Construction (ITcon)*, vol. 27, pp. 571–594, 2022, doi: 10.36680/j.itcon.2022.028.

[35] R. Nagy and Y. Wu, “The industrial safety of food processing in light of operational risks reduction aspects,” *National Security Review*, vol. 2, pp. 92–113, 2022, Accessed: Aug. 13, 2024. [Online]. Available: https://scholar.google.com/citations?view_op=view_citation&hl=es&user=TMm9gZMAAAAJ&citation_for_view=TMm9gZMAAAAJ:wlzmIqt2EaEC.

[36] T. Somogyi and R. Nagy, “Cyber Threats and Security Challenges in the Hungarian Financial Sector,” *Contemporary Military Challenges*, vol. 2022, no. 24/3, pp. 15–29, Oct. 2022, doi: 10.33179/BSV.99.SVI.11.CMC.24.3.1.

[37] T. Somogyi and R. Nagy, “Some impacts of global warming on critical infrastructure protection - heat waves and the European financial sector,” *Insights into Regional Development*, vol. 4, no. 4, pp. 11–20, Dec. 2022, doi: 10.9770/IRD.2022.4.4(1).

[38] S. Wright, J. Barlow, and J. K. Roehrich, “Public-Private Partnerships for Health Services: Construction, Protection and Rehabilitation of Critical Healthcare Infrastructure in Europe,” *Competitive Government: Public Private Partnerships*, pp. 125–151, 2019, doi: 10.1007/978-3-030-24600-6_7/COVER.

[39] O. Mazzeo, A. Longo, and M. Zappatore,

"Cloud Computing and Critical Infrastructure Resilience," pp. 115–126, 2023, doi: 10.1007/978-3-031-28694-0_11/COVER.

[40] R. M. Clark and S. Hakim, "Public–Private Partnerships and Their Use in Protecting Critical Infrastructure," *Competitive Government: Public Private Partnerships*, pp. 1–15, 2019, doi: 10.1007/978-3-030-24600-6_1.

[41] D. Markopoulou and V. Papakonstantinou, "The regulatory framework for the protection of critical infrastructures against cyberthreats: Identifying shortcomings and addressing future challenges: The case of the health sector in particular," *Computer Law & Security Review*, vol. 41, p. 105502, Jul. 2021, doi: 10.1016/J.CLSR.2020.105502.

[42] D. L. Alderson, R. P. Darken, D. A. Eisenberg, and T. P. Seager, "Surprise is inevitable: How do we train and prepare to make our critical infrastructure more resilient?," *International Journal of Disaster Risk Reduction*, vol. 72, p. 102800, Apr. 2022, doi: 10.1016/J.IJDRR.2022.102800.

[43] R. P. Arciniega-Rocha, V. C. Erazo-Chamorro, P. D. Rosero-Montalvo, and G. Szabó, "Smart Wearable to Prevent Injuries in Amateur Athletes in Squats Exercise by Using Lightweight Machine Learning Model," *Information*, vol. 14, no. 7, p. 402, Jul. 2023, doi: 10.3390/info14070402.

[44] V. C. Erazo-Chamorro, R. P. Arciniega-Rocha, A. L. Maldonado-Mendez, P. D. Rosero-Montalvo, and G. Szabo, "Intelligent System For Knee Ergonomic Position Analysis During Lifting Loads," *Acta Technica Napocensis - Series: Applied Mathematics, Mechanics, And Engineering*, vol. 65, no. 3S, pp. 677–684, Jan. 2023, Accessed: Mar. 16, 2023. [Online]. Available: https://atna-mam.utcluj.ro/index.php/Acta/article/view/1950.

Siguranța și securitatea operațională și tehnologică a infrastructurii critice europene în lumina crizelor energetice

Acest studiu explorează siguranța și securitatea operațională și tehnologică a Infrastructurilor Critice (IC) europene în contextul escaladării crizelor energetice. Odată cu ascensiunea Industriei 4.0 și a tehnologiilor digitale - cum ar fi IoT, IA și 5G - sistemele IC au devenit din ce în ce mai interconectate și vulnerabile la amenințări cibernetice, dezastre naturale și tensiuni geopolitice. Lucrarea subliniază importanța Protecției Infrastructurilor Critice (PCI) prin abordări multidisciplinare, managementul riscurilor și colaborare public-privată. Folosind analize de text și studii de caz din lumea reală, autorii examinează impactul deficitului de energie asupra productivității industriale, stabilității economice și bunăstării societății. Cercetarea subliniază nevoia urgentă de strategii robuste și adaptive pentru a proteja IC și a asigura reziliența în fața cererii energetice globale în creștere și a dependențelor digitale.

Ricardo P. ARCINIEGA-ROCHA, PhD. Student, Óbuda University, Donát Bánki Faculty of Mechanical and Safety Engineering, Budapest, Hungary, arciniega.ricardo@uni-obuda.hu, Népszínhaz u. 8, 203920474

Vanessa C. ERAZO-CHAMORRO, PhD. Student, Óbuda University, Donát Bánki Faculty of Mechanical and Safety Engineering, Budapest, Hungary, erazo.vanessa@uni-obuda.hu, Népszínhaz u. 8, 204398956

Szabo GYULA, Assoc. Prof., PhD, Eur. Erg., Óbuda University, Donát Bánki Faculty of Mechanical and Safety Engineering, Budapest, Hungary, szabo.gyula@uni-obuda.hu, Népszínhaz u. 8, 203349199