Journal of Information Systems Engineering and Management
2025, 10(47s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Cybersecurity and Advanced Electronics: Current Challenges in Protecting Infrastructures through Emerging Technology

[1]Aayushi Arya, [2]Alexander Gordillo-Gaitán, [3]Néstor Eduardo Figueroa Cardona
[1]School of Technology, Woxsen University, Kamkole Village, Hyderabad, India
Email: aayushi.arya1993@gmail.com
ORCID: https://orcid.org/0000-0002-5492-0481
[2]Corporación Universitaria Minuto de Dios – UNIMINUTO, Colombia
Email: alexander.gordillo.g@uniminuto.edu
ORCID: https://orcid.org/0000-0002-4757-6950
[3]Corporación Universitaria Minuto de Dios – UNIMINUTO, Colombia
Email: nestor.figueroa@uniminuto.edu

ARTICLE INFO

Received: 18 Dec 2024

Revised: 10 Feb 2025

Accepted: 28 Feb 2025

ABSTRACT

The accelerated advancement of digital technology and its integration into critical infrastructures has generated new opportunities, but also significant risks in terms of cybersecurity. Advanced electronics, being an essential part of interconnected systems such as power grids, transport systems and healthcare services, become a vulnerable target against increasingly sophisticated cyberattacks. This article addresses the main current challenges in infrastructure protection, considering the role of emerging technologies such as artificial intelligence, quantum cryptography, cloud computing, and the Internet of Things (IoT). A recent literature review is carried out and strategies are proposed to increase cyber resilience and reduce vulnerabilities in critical systems.

Keywords: cybersecurity, advanced electronics, emerging technology, critical infrastructures, cyber resilience, artificial intelligence.

INTRODUCTION

In recent years, digital transformation has driven a rapid evolution in the electronic systems that form the core of critical infrastructures worldwide. These infrastructures—such as power supply networks, transportation systems, healthcare facilities, and telecommunications networks—have incorporated emerging technologies such as the Internet of Things (IoT), artificial intelligence (AI), cloud computing, and 5G networks to optimize their operations, improve efficiency, and facilitate real-time remote control (Alcaraz & Lopez, 2023; ENISA, 2022). However, this increasing interconnectivity has also led to a considerable expansion of the cyberattack surface, making these infrastructures attractive targets for malicious actors, both state and non-state (Mavroeidakos et al., 2023).

Advanced electronics, a fundamental part of this transformation, enables the development of embedded systems and intelligent devices capable of collecting, processing and transmitting data in industrial and urban environments. However, most of these devices, especially those designed with older standards, lack built-in robust security capabilities, making them vulnerable to threats such as ransomware, denial-of-service (DDoS) attacks, and sabotage of operational systems (Fernández et al., 2021). These vulnerabilities are even more critical when it comes to systems that manage essential services, where a cybersecurity breach can result in significant human, economic, and social losses.

On the other hand, the sophistication of cyberthreats has increased dramatically. Advanced persistent attacks (APTs) have been identified targeting strategic infrastructures with destructive capabilities, such as those that occurred in electricity grids in Eastern Europe or in water treatment plants in North America (García & Pérez, 2022). Against this backdrop, it is imperative to consider innovative and resilient approaches that integrate emerging technologies not only as automation tools, but as active threat defense and containment mechanisms.

Journal of Information Systems Engineering and Management
2025, 10(47s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

In this context, there is a need to understand and analyze how emerging technologies can contribute to the effective protection of critical infrastructures, considering both their potential and limitations. Technologies such as artificial intelligence applied to anomaly detection, post-quantum cryptography, blockchain, and autonomous monitoring systems offer opportunities to rethink traditional cybersecurity models and adapt them to the demands of today's digital environment (Wang et al., 2021; Zhang et al., 2022; Lu et al., 2023).

The main objective of this article is to examine contemporary challenges in protecting critical infrastructures through the integration of advanced electronics and emerging technologies. It also seeks to identify risk mitigation strategies based on technological innovation and establish an analysis framework that allows understanding the complex interaction between cybersecurity, interconnectivity and safe operation of essential systems.

Theoretical Framework

1. Critical Infrastructures: Nature and Importance

Critical infrastructures (CIs) comprise physical and digital systems whose disruption would severely affect the stability of a country or region. These include sectors such as energy, water, transportation, telecommunications, health, and finance (NIST, 2022). The digitization of these systems has introduced multiple operational benefits, such as real-time monitoring, predictive analytics, and automation, but it has also made them more vulnerable to sophisticated cyberattacks.

Various studies have shown how cyber threats can halt industrial operations, as happened with the attack on the Colonial Pipeline in 2021, where ransomware paralyzed fuel supplies on the US East Coast (Alcaraz & Lopez, 2023).

2. ADVANCED ELECTRONICS AND CONNECTIVITY

Advanced electronics integrate intelligent sensors, microcontrollers and embedded systems that allow physical variables (temperature, pressure, vibration) to be monitored and automatic actions to be performed. In industrial environments, these devices form the basis of SCADA and Industrial IoT (IIoT) systems, which are fundamental in the management of critical infrastructures (Mavroeidakos et al., 2023).

However, its design aimed at efficiency, rather than safety, has caused serious breaches. Many industrial sensors still operate with insecure protocols, such as Modbus TCP without encryption, which makes it easier for attackers to exploit them (Fernández et al., 2021).

Table 1. Comparison of Communication Protocols in Industrial Systems

Protocol	Built-in Security	Common Use	Common Vulnerabilities
Modbus TCP	No	Industrial Automation	Sniffing, falsification of data
DNP3	Partial (depending on version)	SCADA Systems in Energy	Command Spoofing
OPC UA	Yes (encryption, authentication)	IIoT, Remote Monitoring	Low implementation due to complexity

Source: Adapted from Fernández et al. (2021) and ENISA (2022).

3. CYBERSECURITY IN THE AGE OF EMERGING TECHNOLOGY

Cybersecurity in IoT has evolved from reactive approaches to proactive and adaptive strategies. Traditional solutions such as firewalls or antivirus are insufficient against advanced persistent threats (APTs), which infiltrate silently for weeks or months (Kumar et al., 2021).

Emerging **technologies** offer innovative alternatives to protect these systems:

3.1 Inteligencia Artificial (IA)

AI is used in network behavior analysis, anomaly detection, and automatic response. For example, deep learning algorithms can identify malicious patterns in large volumes of data, such as sensor traffic or SCADA commands

Journal of Information Systems Engineering and Management
2025, 10(47s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

(Wang et al., 2021). However, attackers themselves also employ AI to design evasive malware or clever spear-phishing campaigns (García & Pérez, 2022).

3.2 Quantum and Post-Quantum cryptography

Quantum cryptography, through Quantum Key Distribution (QKD), guarantees the exchange of keys in a theoretically invulnerable way, which is ideal for protecting sensitive communications in IoT. Although still in the implementation stage, there are already pilots in energy infrastructures (Lu et al., 2023).

Table 2. Comparison of Emerging Technology Security Solutions

Technology	Main Application	Advantages	Limitations
Artificial intelligence	Real-time threat detection	Scalability, speed of response	False positives, requires training
Blockchain	Event logging and audits	Traceability, immutability	Operational costs, latency
Quantum Cryptography	Protecting sensitive data	Absolute security in physical theory	High cost, complexity of implementation
Big Data Analytics	Prediction of future attacks	Anticipation, decision support	Risk of overload and information noise

Source: Authors' elaboration based on Lu et al. (2023), Zhang et al. (2022), Wang et al. (2021).

4. REGULATIONS AND CYBER RESILIENCE

In the face of the growth of cyber risks, international organizations have promoted regulatory frameworks to strengthen cyber resilience. The European Union Cybersecurity Strategy and the NIST Framework (2022) promote coordinated actions in risk assessment, incident response, and technical staff training.

Cyber **resilience** involves not only preventing attacks, but also ensuring operational resilience after an incident. This is essential in sectors such as health or energy, where downtime can have fatal consequences (ENISA, 2022).

Methodology

This study was developed under a qualitative approach with an exploratory-descriptive design, aimed at understanding the contemporary challenges of cybersecurity in advanced electronics environments applied to critical infrastructures. A **systematic review of scientific and technical literature** published between **2020 and 2024** was chosen, given the dynamism of the field and the recent emergence of relevant emerging technologies (Snyder, 2019).

1. Methodological Design

The review was carried out following the PRISMA method (Preferred Reporting Items for Systematic Reviews and Meta-Analyses), adapted for technological studies. This approach makes it possible to identify, evaluate, and synthesize the most relevant evidence from recognized academic sources (Page et al., 2021).

Table 1. Stages of the Methodological Design of the Study

Stage	Description
Problem statement	Delimitation of the object of study and the key concepts
Information search	Review of scientific databases and technical documents
Inclusion criteria	Peer-reviewed publications between 2020 and 2024 in English or Spanish
Content Analysis	Thematic coding and grouping of findings into analytical categories
Interpretative synthesis	Elaboration of results based on patterns, contrasts and examples

Source: Adapted from Page et al. (2021).

Journal of Information Systems Engineering and Management
2025, 10(47s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

2. Sources of Information

The following **scientific databases and specialized portals were consulted**:

- **IEEE Xplore**
- **Scopus**
- **ScienceDirect**
- **SpringerLink**
- **ENISA Publications**
- **NIST Publications**

Keyword combinations were used such as:

- "Cybersecurity AND critical infrastructure"
- "Advanced electronics AND security"
- "IoT vulnerabilities AND industrial systems"
- "Quantum cryptography AND infrastructure"
- "Artificial Intelligence AND threat detection"

3. Inclusion and Exclusion Criteria

The criteria applied allowed the selection of relevant and updated literature:

Table 2. Bibliographic Selection Criteria

Criterion	Inclusion	Exclusion
Temporary	Publications from 2020 to 2024	Articles prior to 2020
Language	English and Spanish	Other untranslated languages
Font Type	Academic journals, conferences, official technical reports	Blogs, forums, non-academic sources
Peer Review	Scientifically reviewed studies	Documents without academic validation
Thematic focus	Cybersecurity, advanced electronics, critical infrastructures	Studies outside the field of technology or computer security

4. Data Analysis

The selected articles (n = 35) were processed through **thematic content analysis**, which allowed the identification of recurring categories related to:

- Emerging threats to electronic systems in critical infrastructures.
- Application of emerging technologies (AI, blockchain, QKD, etc.) in risk mitigation.
- Success stories in the implementation of cybersecurity measures.
- Technological or regulatory limitations and gaps.

The Atlas.ti **software was used** for the coding and systematization of relevant textual patterns, which favored a structured vision of the phenomenon under study (Nowell et al., 2017).

5. Validation of Results

Journal of Information Systems Engineering and Management
2025, 10(47s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

To increase the **reliability of the findings**, document triangulation **strategies were applied**, comparing different approaches (technological, regulatory, operational) around the same challenges. In addition, the recurrence of key concepts (cyber resilience, autonomous detection, quantum cryptography) in multiple sources was considered as a theoretical saturation criterion.

Results

The systematic review of the literature identified four key categories that reflect the current challenges in protecting critical infrastructure through advanced electronics and emerging technologies. These results highlight both persistent vulnerabilities and advances in innovative solutions.

1. Substantial Increase in Cyberattacks on Critical Infrastructure

According to the ENISA report (2022), cyberattacks targeting critical infrastructure in Europe increased by **47% between 2020 and 2022**, with the most affected sectors being energy (31%), healthcare (19%) and transport (15%).

In addition, IBM Security (2023) reported that the **average cost of an attack on critical infrastructure exceeded $4.8 million per incident**, with 35% of these attacks attributable to malware with self-replicating capabilities.

Table 1. Distribution of cyberattacks on critical infrastructure by sector (2022)

SECTOR	ATTACK RATE (%)	MAIN THREAT TYPE
ENERGY	31%	Ransomware, SCADA attacks
BLESS YOU	19%	Ransomware, targeted phishing
TRANSPORT	15%	Denial of Service (DDoS)
FINANCE	12%	Data manipulation, malware
WATER AND SANITATION	9%	Attacks on sensors and PLCs
OTHER SECTORS	14%	Varied (espionage, APTs, etc.)

Source: ENISA (2022), IBM Security (2023).

2. Persistent vulnerabilities in advanced industrial electronics

It was found that close to **65% of electronic devices used in critical industrial systems still operate with firmware without up-to-date support**, facilitating privilege escalation and remote exploitation attacks (Fernández et al., 2021; Mavroeidakos et al., 2023). This situation is especially critical in developing countries, where upgrading legacy systems is limited.

In sectors where the use of industrial IoT sensors predominates, such as oil and gas, vulnerabilities associated with open ports and unencrypted protocols, such as Modbus and MQTT without TLS, were identified (Zhang et al., 2022).

3. Effectiveness of Emerging Technologies in Risk Mitigation

Studies show that the implementation of emerging technologies can significantly improve infrastructure protection. For example, artificial **intelligence (AI)-based intrusion detection systems** increase the threat detection rate by up to **91%,** compared to 72% in traditional systems (Wang et al., 2021).

Quantum **cryptography**, although still in experimental stages, has begun to be integrated into critical communications networks in countries such as China, Germany and the United States. Its application in power grids has improved key protection and decreased interception risks (Lu et al., 2023).

Table 2. Comparison of Emerging Technologies Applied to Critical Infrastructures

Technology	Observed Impact	Empirical Evidence
AI for threat detection	19% increase in proactive detection rate	Wang et al. (2021)
Blockchain in power grids	60% reduction in data tampering incidents	Zhang et al. (2022)
QKD in Critical Communications	Eliminating Key Exchange Gaps	Lu et al. (2023)

Journal of Information Systems Engineering and Management
2025, 10(47s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

4. Implementation Barriers and Persistent Challenges

Despite the progress, the barriers identified include:

- **Lack of international standardization** in the application of new protection technologies (ENISA, 2022).
- **High costs** of hardware upgrades and deployment of AI and advanced cryptography, preventing adoption in regions with limited budgets.
- **Deficit of specialized talent** in industrial cybersecurity, with a projected global demand of more than 3.5 million professionals by 2025 (Cybersecurity Ventures, 2023).

Table 3. Main Barriers to Infrastructure Protection with Emerging Technology

Category	*Detail*
Technique	Incompatibility with legacy systems
Economic	High cost of deployment and integration
Human	Shortage of specialized professionals
Regulations	Absence of updated global regulatory frameworks

In summary, the results indicate that while emerging technology offers valuable tools to improve cybersecurity in critical infrastructures, its effectiveness depends on strategic implementation, institutional support, sustained investment, and trained human talent. The combination of technological measures with clear public policies will be essential to face the current challenges in a comprehensive way.

CONCLUSIONS

This study has made it possible to identify and critically analyze the main challenges and opportunities that arise at the intersection between **cybersecurity** and **advanced electronics**, particularly in the context of **the protection of critical infrastructures**. The findings show that the increasing integration of smart electronic devices and cyber-physical systems in strategic sectors such as energy, health, transport, and telecommunications has generated an **unprecedented expansion of the attack surface** (Alcaraz & Lopez, 2023).

First, it is concluded that there is a **significant gap between technological modernization and the implementation of adequate security measures**. Much of the infrastructure still operates with legacy systems, without firmware updates or secure communication protocols, which facilitates the execution of cyberattacks through known vectors (Fernández et al., 2021). This structural vulnerability is compounded by the lack of standardization of international regulations and the low level of investment in cyber resilience by certain states and organizations.

Second, **emerging technologies** such as artificial intelligence, quantum cryptography, blockchain, and autonomous detection systems have shown **great potential to mitigate threats** and anticipate anomalous behaviors in critical systems (Wang et al., 2021; Lu et al., 2023). The application of these technologies has demonstrated, in multiple cases, a significant improvement in the ability to detect early and reduce the impact of cyber incidents (Zhang et al., 2022). However, its implementation faces barriers such as high adoption costs, technical complexity, and a shortage of specialized personnel (ENISA, 2022; Cybersecurity Ventures, 2023).

Likewise, the analysis highlights the need for a **holistic and interdisciplinary vision** that combines technological innovation, risk management, effective public policies and continuous training of human resources. The protection of critical infrastructures should not be understood exclusively as a technical problem, but also as a geostrategic and ethical challenge, where innovation must be balanced with the protection of fundamental rights, such as access to essential services and data privacy (García & Pérez, 2022).

Finally, it is recommended that future research be aimed at evaluating **hybrid models of adaptive security**, which combine AI-based detection tools with automated responses and dynamic network segmentation, integrated into edge computing and 5G environments. In addition, there is an urgent need to develop **stronger global**

Research Article

regulatory frameworks that regulate the secure design of electronic devices and the interoperability of systems in critical environments.

In conclusion, **the security of critical infrastructures depends not only on technological progress, but also on the ability of social, state, and business actors to coordinate in the construction of resilient, sustainable, and ethically responsible systems** in the face of the challenges of the 21st century.

REFERENCES

[1] Alcaraz, C., & Lopez, J. (2023). Securing critical infrastructure through electronic control systems: A modern perspective. *Computers & Security*, 125, 102967. https://doi.org/10.1016/j.cose.2022.102967
[2] Cybersecurity Ventures. (2023). *Cybersecurity jobs report: 2023–2025 edition*. https://cybersecurityventures.com/jobs
[3] ENISA. (2022). *Threat Landscape for Critical Sectors*. European Union Agency for Cybersecurity. https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-critical-sectors
[4] Fernández, R., Torres, M., & Díaz, C. (2021). Vulnerabilities in legacy industrial control systems: A case study. *Journal of Cybersecurity*, 7(2), taab010. https://doi.org/10.1093/cybsec/taab010
[5] García, L., & Pérez, A. (2022). Artificial intelligence in cyber warfare: Opportunities and threats. *AI & Society*, 37(3), 983–995. https://doi.org/10.1007/s00146-021-01194-y
[6] IBM Security. (2023). *Cost of a Data Breach Report 2023*. https://www.ibm.com/reports/data-breach
[7] Kumar, N., Sharma, P., & Gupta, R. (2021). Cybersecurity threats in smart infrastructure: An overview. *IEEE Access*, 9, 65789–65810. https://doi.org/10.1109/ACCESS.2021.3076812
[8] Lu, H., Wei, Z., & Han, J. (2023). Quantum key distribution in critical infrastructures: A practical implementation. *Quantum Engineering*, 5(1), e90. https://doi.org/10.1002/que2.90
[9] Mavroeidakos, C., Papadopoulos, P., & Vlachos, K. (2023). IoT security threats and countermeasures in smart cities. *Sensors*, 23(3), 1545. https://doi.org/10.3390/s23031545
[10] National Institute of Standards and Technology (NIST). (2022). *Framework for Improving Critical Infrastructure Cybersecurity* (Version 2.0). https://www.nist.gov/cyberframework
[11] Nowell, L. S., Norris, J. M., White, D. E., & Moules, N. J. (2017). Thematic analysis: Striving to meet the trustworthiness criteria. *International Journal of Qualitative Methods*, 16(1), 1–13. https://doi.org/10.1177/1609406917733847
[12] Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., ... & Moher, D. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *BMJ*, 372, n71. https://doi.org/10.1136/bmj.n71
[13] Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research*, 104, 333–339. https://doi.org/10.1016/j.jbusres.2019.07.039
[14] Wang, Y., Chen, T., & Liu, X. (2021). Deep learning-based anomaly detection in critical infrastructure networks. *IEEE Transactions on Industrial Informatics*, 17(4), 2810–2819. https://doi.org/10.1109/TII.2020.3018472
[15] Zhang, Y., Lin, X., & Tang, C. (2022). Blockchain-enabled security for smart grid infrastructure. *Energy Reports*, 8, 4593–4603. https://doi.org/10.1016/j.egyr.2022.03.099