OPEN ACCESS **Scientific Letters**

IV 1H-TOXRUN INTERNATIONAL CONGRESS 2025 | 08-09 MAY, 2025 Porto, Portugal

Poster 17

Cyberattacks on critical infrastructures: the role of Forensic Sciences in prevention and investigation

Miguel Morgado [1], Carla Malafaya [1], Manuela Oliveira [2,3,4], Luís Fernandes [2,3,4], Áurea Madureira-Carvalho [2,3] and Rui Azevedo [2,3,*]

[1] Maia High School, Avenida Luís Camões Maia 4470-322, Portugal
[2] Associate Laboratory i4HB - Institute for Health and Bioeconomy, University Institute of Health Sciences - CESPU, 4585-116 Gandra, Portugal
[3] UCIBIO - Research Unit on Applied Molecular Biosciences, Forensic Sciences Research Laboratory, University Institute of Health Sciences (1H-TOXRUN, IUCS-CESPU), 4585-116 Gandra, Portugal
[4] OSI – Homeland Security Observatory, 4585-116 Gandra, Portugal

* Correspondence: rui.azevedo@iucs.cespu.pt

Abstract

Background: Critical infrastructures (e.g., national security, energy systems, transport systems/supply chain, health, and telecommunications) (fig. 1) have been the target of constant cyber-attacks that debilitate the population's sense of security and have had profound economic, social, and public safety impacts [1,2]. Also, cyber-physical systems in smart cities face complex challenges that require robust cyber-resilience and digital forensic incident response strategies [3]. **Objective:** To understand the role of digital forensic techniques in preventing and investigating these cyberattacks. **Methods:** A systematic literature review was carried out (Association of Computing Machinery, PubMed, Scopus and IEEExplore) of articles published between 2020 and 2025, using the keywords: “critical infrastructure”, “cyberattack”, “digital forensics” and “incident response”. The papers obtained were selected based on predefined inclusion criteria (thematic relevance, scientific rigor, and date of publication) and exclusion criteria (articles outside the specified period and not peer-reviewed). **Results:** Initially, 146 articles were identified, 45 of which were included in the review after applying the inclusion/exclusion criteria. The main results show a growing use of advanced digital forensic investigation techniques, including automated and artificial intelligence tools (examples: facial recognition with AI, genetic analysis with machine learning, language analysis, and behavioral profiling), for the rapid identification of incidents and proactive prevention. Methods for forensic analysis in SCADA systems, smart grids, computerized hospital systems, and telecommunications were highlighted. The literature also pointed to significant challenges in preserving digital evidence and the difficulty in attributing authorship and accountability for attacks. The results show significant advances in digital forensic techniques applied to protecting and investigating attacks on critical infrastructures, primarily through AI and automation. However, vital and considerable challenges persist (e.g., the systems' complexity, threats' continuous evolution, and the legal difficulties associated with digital evidence collection and validation). **Conclusions:** Investments in specialized research and development will strengthen the ability of forensic teams to respond to emerging cyber threats and ensure the security and resilience of critical infrastructures.

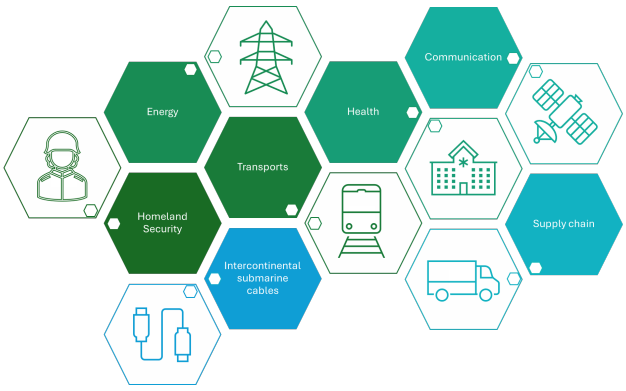

Figure 1. Examples of critical structures.

Keywords: digital awareness; forensic analysis; resilience

Acknowledgments/Funding

This research received no external funding.

References

1. Bellamkonda, S. Cybersecurity in critical infrastructure: Protecting the foundations of modern society. *Int J Commun Netw Inf Secur* **2020**, *12*, 273-280.
2. Dawson, M. et al. Understanding the challenge of cybersecurity in critical infrastructure sectors. *Land Forces Acad Rev* **2021**, *26*, 69-75, doi: 10.2478/raft-2021-0011.
3. Ahmadi-Assalemi, G. et al. Cyber resilience and incident response in smart cities: A systematic literature review. Smart Cities **2020**, *3*, 894-927, doi: 10.3390/smartcities3030046.