Aleksandar IVANOVIĆ,
Doctor of Law (PhD), Professor,
Professor University «Mediterranean» Podgorica, Montenegro
ORCID: https://orcid.org/0000-0002-8186-0883
e-mail: ialeksandar@t-com.me

DOI: https://doi.org/10.32620/pls.2025.8.44

THE ROLE OF FORENSICS AND CRIMINAL SCIENCE IN CRITICAL INFRASTRUCTURE PROTECTION

Abstract. *The article examines the pivotal role of forensic science and criminology in safeguarding critical infrastructure, which encompasses essential sectors such as energy, water supply, telecommunications, transportation, healthcare, and finance. These infrastructures are increasingly vulnerable to hybrid threats – ranging from cyberattacks and insider sabotage to physical destruction – due to their reliance on digital technologies and interconnected systems. The author emphasizes that digital, technical, and physical forensics are indispensable for incident analysis, evidence collection, and system integrity, while criminology contributes through behavioral analysis, intelligence gathering, and criminal investigations. The synergy between these disciplines enables effective threat mitigation, policy enhancement, and personnel training. In the context of global insecurity and evolving risks, the integration of forensic and criminological approaches is presented as a cornerstone of national resilience and security strategy.*

Keywords: *critical infrastructure, national security, forensic science, digital forensics, SCADA systems, IoT forensics, hybrid threats, insider threats, criminology, behavioral analysis, cybercrime, intelligence operations, preventive measures, security policy.*

Introduction.

The value of Critical Infrastructure protection as part of the National Security of a country includes and intertwines 'Assets, Systems and Networks' whose damage, disruption and/or destruction will have serious consequences for the protection of the 'Essential Functions' of the country, such as the provision of 'Health, Public Safety and Economic Activities' and the maintenance of order in the country. Examples of such sectors are Electricity, Water Supply and Sewerage, Telecommunications, Transport, Healthcare, Finance, etc., these sectors are of paramount importance. Infrastructures are of strategic importance, which makes them susceptible to a wide range of threats, from technological system failures and natural disasters, cyberattacks, industrial espionage, terrorist acts and internal supplies. Therefore, forensics and criminal science have a key importance in preserving and maintaining the integrity, functionality and security of these systems. They provide the basis for identification and analysis of threats, collection and processing of evidence, detection of perpetrators and establishment of preventive measures.

The goal of this presentation is to show the contributions of forensics and criminology in the protection of critical infrastructure and how their joint synergy enables the building of a resilient and secure society that responds to contemporary challenges. Definition, significance and vulnerabilities of critical infrastructure.

Results and Discussion.

Critical infrastructure is the basis of everyday life and the functioning of every modern society. Its protection is the priority of every state, because any interference in its functioning causes far-reaching consequences. However, it is precisely its complexity and unique connection that makes it increasingly vulnerable. The following text mentions the challenges that critical infrastructure brings.

1.1. Increased dependence on digital technologies. Industrial control systems (ICS), SCADA platforms, automated processes, cloud services and communication systems are indispensable in today's infrastructure. Connecting the Internet of Things (IoT) in energy, transport and healthcare opens up a large number of new entry points for attackers.

1.2 Hybrid Threats Modern threats are neither exclusively physical nor digital – more often than not they come in both forms. For example, cyberattacks can cause physical damage (e.g. by taking over power/electricity systems).

1.3 Insider Threats Employees and collaborators with access to sensitive information or systems are potential threats. Security incidents are often the result of these insider threats – either knowingly or unknowingly.

2. The Role of Forensics in Critical Infrastructure Protection

Forensics is the discipline of collecting, analyzing, and interpreting traces, evidence, and information that can be used to determine the causation of incidents. In the critical infrastructure field, digital and technical forensics are the most important, although other conventional disciplines also play a significant role in various situations.

2.1 Digital forensics of networks and systems Digital forensics enables analysis of cyber attacks, detection of malicious software, reconstruction of events and collection of logs, network packets and other digital evidence.

2.2. Forensic analysis of ICS and SCADA systems ICS and SCADA systems usually use outdated protocols and do not meet modern security standards. Their forensic analysis, however, is not trivial and they are highly specialized.

2.3. IoT Device Forensics IoT devices produce massive amounts of data, and forensic analysis is required to detect unauthorized access, firmware modifications, and changes to embedded physical controls.

2.4. Physical Forensics When an industrial plant is sabotaged and there is a fire or destruction of equipment, different branches of forensics are applied: fire engineering and forensics, chemistry, ballistics, etc.

3. The role of forensics in the protection of critical infrastructure

Criminology is a field of science that studies the methods of detecting, investigating and proving crimes. Within the framework of critical infrastructure, it plays a crucial role in threat assessment, identification of perpetrators and prevention of illegal actions, of which the following would be highlighted:

3.1. Analysis of criminal behavior patterns Criminalists study the motives, behavior patterns, resources and abilities of a potential attacker.

3.2. Operational-intelligence work includes gathering information about criminal and terrorist groups, risk assessment and attempts to prevent attacks.

3.3. Incident Investigations Criminal investigators conduct investigations into cases of sabotage, cyber crimes, data theft, terrorism and other actions directed against critical infrastructure.

4. Synergy of forensics and criminology

The implementation of forensics and criminology in the protection of critical infrastructure, combined with their use, can provide us with effective and efficient responses in case of incidents of critical infrastructure, in the phase of: - prosecution of perpetrators, - improvement of security policies, and - employee education.

Conclusion.

Forensics and criminology represent the two most important pillars for the protection of critical infrastructure. Their role is of paramount importance in the modern era of hybrid threats and cyber risk with global insecurity.

Bibliographic references:

1. Smith, J. (2020). Critical Infrastructure Protection: Theory and Practice. New York, 2020.

2. Springer. Johnson, M. & Lee, R. (2019). Forensic Science in Cybersecurity. London, 2019.

3. Routledge. Brown, A. (2021). Industrial Control Systems and Security Challenges. Berlin, 2021.

4. De Gruyter. Wilson, T. Cyber Threats and Critical Infrastructure. Oxford: Oxford University Press, 2018.

5. Davis, K. Digital Forensics and Evidence Handling. Chicago: University Press, 2022.

A. Ivanović

The role of forensics and criminal science in critical infrastructure protection.

Citation example:

Ivanović A. The role of forensics and criminal science in critical infrastructure protection. Propilees of Law and Security, 2025. No. 8. P. 186-187. DOI: https://doi.org/10.32620/pls.2025.8.44.