NBP. Nauka, bezbednost, policija
Published by
University of Criminal Investigation and Police Studies
2026, Vol. 31, Issue 1, pp. 95–111
https://doi.org/10.5937/nabepo31-60802
Review Essay

Ecoterrorism and Cyberattacks vs. Critical Infrastructure: Counterintelligence and Security Aspects

Dragan Živaljević[1], Nevena Gavrić[2]
National Security Academy, Belgrade, Serbia

Submitted: 2025-08-13 • Accepted: 2025-12-24 • Published: 2026-01-08

Abstract: Critical infrastructure encompasses systems and resources essential to the functioning of the state and its protection consequently stands at the pinnacle of counterintelligence and security priorities. Amid increasingly intensive and complex forms of hybrid threats, the vulnerability of such systems becomes more pronounced – particularly in the domains of cyber-attacks and eco-terrorist acts, as emergent forms of asymmetric threats. Of particular concern is the employment of sophisticated methods of espionage, cyber intrusions and subversive activities, all of which necessitate a strategically oriented and integrated counterintelligence response. In addition to conventional and digital security risks, growing attention must be directed towards the phenomenon of eco-terrorism – that is, the activities of radical environmental groups which, under the guise of environmental protection, carry out attacks targeting infrastructure of vital importance. Cyber threats, including intrusions into operational networks, data destruction and manipulation of control systems, constitute a parallel dimension of security vulnerability, one that challenges the response capacity of traditional protection systems. This paper examines the intersection between eco-terrorism, cyber-attacks and the counterintelligence protection of critical infrastructure, with a particular focus on identifying vulnerabilities, evaluating the effectiveness of the existing measures and analysing the role of institutional actors in the prevention, detection and response to such threats. Special attention is paid to the challenges of intersectoral coordination and the pressing need to improve both national and international regulatory and operational frameworks. Drawing upon an analysis of current security strategies and selected case studies, the paper argues that the effective safeguarding of critical infrastructure is achievable solely through a multidisciplinary and comprehensive approach – one that integrates counterintelligence capabilities, technological innovation and international cooperation. The findings of the research offer concrete recommendations for the reform and enhancement of legal and institutional mechanisms, with an emphasis on proactive engagement, situational awareness and adaptive crisis response to the threats emerging from eco-terrorist and cyber domains. The contribution of this study lies in its critical examination of the security aspects of contemporary threats to critical infrastructure, offering insights relevant both to the academic community and to decision-makers engaged in the formulation of national and international security policy.

Keywords: critical infrastructure, counterintelligence protection, national security, cyber threats, hybrid warfare.

1 zivaljevic@gmail.com • https://orcid.org/0009-0005-3829-4344 • Associate Professor.
2 Corresponding author: nevena.gavric2020@gmail.com • Phone: +381 63 34 14 07 • Teaching Assistant.

eISSN 2620-0406

INTRODUCTION

In contemporary security discourse, the protection of critical infrastructure (CI) occupies a central position, necessitating its systematic definition, the articulation of its strategic value and an examination from both counterintelligence and general security paradigms.

The primary objective of this paper is to offer a comprehensive analysis of the security risks and threats to which CI is exposed, with particular emphasis on the role of counterintelligence protection in preserving its integrity and functionality. The authors focus on identifying dominant security challenges, evaluating institutional responses, and formulating recommendations for improving protection measures. Furthermore, legal and regulatory mechanisms governing this area are examined, as well as international standards relevant to crisis management in security contexts.

The relevance of the topic stems from the growing exposure of states to complex hybrid threats, wherein traditional forms of violence intersect with advanced, covert and unconventional methods of operation such as cyber operations, cognitive manipulation techniques and information warfare. CI is becoming increasingly vulnerable within the context of globalisation and exponential technological progress, both of which provide space for the activities of diverse actors – from state and non-state entities to transnational criminal and terrorist networks. Cyber threats, eco-terrorism and subversive activities represent just some of the forms of endangerment faced by modern security systems. The effective protection of CI requires the development of flexible and resilient strategies, the continual improvement of security protocols and institutionalised cooperation between public and private sectors.

The methodological approach of this study is grounded in an analytical-synthetic framework that integrates theoretical perspectives and empirical insights within the field of CI protection. The principal research method is qualitative analysis of relevant literature, legal acts and concrete case studies. In addition, comparative and descriptive methods, as well as content analysis, have been employed to shed precise light on key challenges and generate realistic and applicable recommendations.

The structure of the paper is organised into several thematic sections. The first section explores the concept, importance and resilience of CI, with an analysis of international standards and national protection strategies. The second section centres on contemporary threats, with hybrid forms of endangerment such as cyber-attacks and eco-terrorism taking precedence. The third segment addresses the role of counterintelligence structures in protecting CI, examining their methods, tools and operational challenges. The fourth section assesses the legal and institutional framework, while the fifth outlines examples of best practices. The final section presents the study's key findings, along with proposed guidelines for improving CI protection strategies.

The clearly defined methodological structure of the paper ensures analytical precision and lays the foundation for further theoretical and applied research in the security field. It is anticipated that the findings will contribute to the development of national security policy, the enhancement of the legal framework and the strengthening of institutional resilience in the face of current and future threats.

CI RESILIENCE AND VULNERABILITY

Definition, Importance, and CI Sectors

The conceptual and terminological apparatus distinguishes between the terms *vulnerability* and *resilience*. Vulnerability refers to the exposure to danger, destruction or damage, while resilience denotes the capacity to resist influence, pressure or change – something that is directly supported by counterintelligence protection mechanisms. Although the concept of CI resilience is not explicitly referenced in Serbian legislation, research confirms its importance as a defining characteristic of critical infrastructure. Consequently, resilience is frequently embedded within the security strategies of economically stable nations and is aimed at fostering the adaptive capacities of individuals, communities or systems in order to maintain an acceptable level of functionality, structure and identity (Barasa et al., 2018).

In the Republic of Serbia, the legal framework for the identification and protection of CI was established in 2018 through the Law on Critical Infrastructure, which defines CI as "systems, networks and facilities or parts thereof, whose interruption of functioning or disruption in the provision of goods or services may have serious consequences for national security, human life and health, property, the environment, public safety, economic stability, or may otherwise jeopardise the functioning of the Republic of Serbia". The sectors identified as CI include: energy, transport, water and food supply, healthcare, finance, telecommunications and information technologies, environmental protection and the functioning of public authorities (Article 4 of the Law on Critical Infrastructure) (Zakon o kritičnoj infrastrukturi, 2018).

CI constitutes a complex, globally distributed and interdependent system whose scale is such that absolute and comprehensive protection at all times and in all locations is realistically unattainable. Consequently, there remains a tangible likelihood that certain terrorist acts targeting these strategic assets may succeed in breaching even the most sophisticated security barriers. Within this context, a core component of any effective and comprehensive CI protection strategy lies in the system's developed capacity to mitigate the consequences of potential attacks through timely adaptation, damage minimisation, efficient emergency management and the ability to recover swiftly and in a coordinated manner. This approach – which emphasises resilience and recovery is recognised as a foundational strategic element within security policies and doctrines adopted at the international level, including in the positions articulated by the United Nations Security Council (2017).

Simeunović (2009) highlighted the significance of international transport as CI and its vulnerability to terrorism, framing it as a serious security challenge. The author further emphasised the necessity of international cooperation in combating terrorism, stating that Serbia is doing all within its power by striving to build cooperative bridges and maintain active engagement with other states in this common fight.

The National Infrastructure Advisory Council (NIAC), the leading advisory body on CI security in the United States, underscores the importance of infrastructure resilience defined as the ability of CI to reduce the magnitude and/or duration of disruptive events. The effectiveness of CI resilience depends on its capacity to anticipate, absorb, adapt to, and/or rapidly recover from such disruptive incidents (National Infrastructure Advisory Council [NIAC], 2009).

Additionally, NIAC is tasked with enhancing public-private sector cooperation and partnerships in securing CI and provides guidance on policies and strategies, ranging from risk assessment and management to information sharing, protective strategies and clarification of roles and responsibilities between public and private actors. Such partnerships are essential for effective communication and coordination in resilience-building, protection and recovery efforts (NIAC, 2009).

Key Threats: Hybrid Threats, Cyberattacks, Eco-Terrorism

Hybrid Threats

Hybrid threats encompass a combination of conventional and unconventional attack methods, often involving propaganda campaigns, economic pressure and cyber operations aimed at destabilizing state institutions. These threats are particularly prominent in geopolitical contexts, where both state and non-state actors employ disinformation and cyber sabotage as part of broader hybrid warfare strategies (Costa, 2021).

The Community of Interest for Vulnerabilities and Resilience at the European Centre of Excellence for Countering Hybrid Threats concluded, after a two-year assessment, that asymmetric techniques such as cyber tools, covert special operations, disinformation dissemination, political agitation and economic instruments, when combined with the vulnerabilities of modern CI, constitute a new category of threat. It was further established that a hybrid adversary may gain a significant advantage in conflicts by targeting CI in countries that rely on open market economies and transparent democratic decision-making processes (Savolainen, 2019). Cyber attacks and the cyber battlefield have become an integral component of hybrid warfare, representing one of the most frequent and most effective non-kinetic means of assault against a society and the state. Over the past decade, this form of warfare has been conducted among the world's most developed and powerful states, primarily between the United States and China, while the long-standing conflict between Russia and Ukraine has been particularly marked by the conduct of hybrid warfare, with a pronounced emphasis on cyber operations (Putnik, 2023).

Cyberattacks

Cyberattacks represent one of the most significant threats to CI due to their potential to compromise ICT systems, financial institutions and energy networks. According to the National CERT of the Republic of Serbia (National Center for the Prevention of Security Risks in ICT Systems), the number of cyberattacks on CI institutions (specifically operators of ICT systems of special importance) has been steadily increasing. The most frequent incidents include: unauthorised data collection (port scanning), intrusion attempts (credential harvesting), fraud (with phishing accounting for the majority of reports) (Nacionalni CERT Republike Srbije, 2022).

One of the most serious incidents in this context was the cyberattack on Ukraine's power grid in 2015, which resulted in widespread power outages affecting several hundred thousand citizens (SANS Institute, 2016). This attack not only disrupted the daily functioning of large urban centres and vital services, but also had significant economic repercussions. Forced to rely on alternative and more expensive sources of energy, Ukraine experienced a

short-term surge in electricity prices. This situation exemplifies the deep interdependence between energy infrastructure and macroeconomic stability, considering that the energy sector constitutes one of the fundamental pillars of modern state economies. Temporary interruptions in energy supply, as well as the long-term degradation of infrastructure capacities, may lead to serious disruptions in economic activity, reduced productivity, increased unemployment rates and mounting inflationary pressures (Venkatachary et al., 2024). For these reasons, cyberattacks targeting the energy sector must be recognised as multidimensional threats, not only from a technical or security standpoint, but also within a broader socio-economic context.

Another notable example of an industrial cyberattack occurred in 2014, when a steel plant in Germany was targeted. According to the official report by the German Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik – BSI), attackers exploited phishing techniques and advanced social engineering to infiltrate the factory's IT system and gain access to its internal network. The initial breach occurred via the administrative network, enabling a further incursion into the operational systems controlling industrial equipment. This lateral movement within the network led to frequent malfunctions of various control system components, severely impairing the functionality of the production process. The most significant damage occurred within the blast furnace control system, which operators were unable to shut down safely or in a timely manner. As a result, substantial technical damage ensued, categorised by BSI as "massive damage to the plant". In this case, the human factor proved crucial, as certain employees had enabled so-called "backdoors", allowing for the installation of malware and the compromise of the entire network (Domović, 2017).

A prominent example of cyber weaponry specifically designed to sabotage industrial control systems is Stuxnet, discovered in 2010 and developed to disrupt Iran's nuclear programme. Stuxnet was an exceptionally sophisticated malicious software targeting Siemens industrial control systems used by Iran. It is believed to have significantly delayed Iran's nuclear activities, inaugurating a new era of cyber warfare by demonstrating the potential for digital attacks to yield physical consequences (Jovanović, 2025).

There is also the example from April 2001, when the FBI investigated the hacking of a Californian test grid by the Honker Union of China (HUC). The case was widely dismissed at the time as media hype, but in 2007 the CIA informed industry leaders that not only was a tangible hacker threat to such CI possible, but that it had, in fact, already occurred (Geers, 2009). These types of incidents clearly underline the imperative to strengthen cybersecurity across critical sectors.

Domović (2017) identifies several systemic issues that facilitate cyberattacks and outlines standard, though still inadequate, countermeasures:

– *Incomplete procedures*. Security protocols must be comprehensive to prevent circumvention via procedural vulnerabilities, commonly referred to as "security gaps".
– *Insufficient employee education on social engineering threats*. Continuous awareness-raising is essential, covering topics such as social engineering tactics, data protection, information system security and, crucially, the importance of protecting CI as a whole.

– *Inadequate coordination with external contractors*. Clear service-level agreements (SLAs) must be established, defining the operational framework in accordance with the defensive strategies specific to each piece of critical infrastructure.

Eco-terrorism

Eco-terrorism is a form of extremism based on attacks against infrastructure with the aim of drawing attention to environmental issues or achieving political goals related to environmental protection, where sabotage and disruption of industrial facilities are the most commonly used methods by radical environmental groups in pursuit of their objectives.

Eco-terrorism is used to describe acts of violence, threats, sabotage, vandalism, intimidation of people and destruction of property, undertaken in the name of environmental preservation. The primary objective of eco-terrorists or environmental extremists is to halt the exploitation of natural resources and draw public attention to environmental protection and related issues (Chalecki, 2002).

Unlike other methods used by extremists, environmental tactics – such as contaminating water supplies or starting fires – can be rapidly planned, requires minimal technical expertise to execute and are more difficult to detect, while causing significant consequences for people, infrastructure and the economy. Moreover, militant organisations including ISIS, Hezbollah and Al-Qaeda have openly promoted the strategy of "environmental jihad" (Somers, 2019). There have been many eco-terrorist attacks over the past 20 years, but some of the more significant examples include ISIS's control of the Fallujah Dam in 2015 and the subsequent flooding downstream as a means of intimidating the Iraqi population deemed disloyal; the destruction of Somali civilian water supplies by Al-Shabaab in 2014; the sabotage of the Iran-Turkey oil pipeline in 2020, which resulted in USD 250 million in damages and lost revenue; the destruction of the Catatumbo oil pipeline in Colombia in 2015 by the Revolutionary Armed Forces of Colombia; and the use of kites and balloons by Hamas in 2018 to ignite fires on Israeli agricultural land, among others (Chalecki, 2024).

Given that environmental crimes cross the borders of the state in which they are committed, states are united in the view that harmonised and coordinated cooperation is essential, both in combating eco-terrorism and other criminal offences in the field of environmental protection. In this regard, Stojanović and Bodrožić (2025) highlight the importance of the Directive (EU) 2024/1203 on the protection of the environment through criminal law of April 2024, which sets the principles to be followed by the EU member states and candidate countries (for EU membership) in the field of criminal law relating to environmental protection.

In Serbia, eco-terrorist activities are still rare, but there is potential for their increase in the context of possible instrumentalisation of elements of environmental protests, due to the heightened public awareness of environmental issues and intensified activity in that area. State authorities recognise the need to monitor these risks and to develop mechanisms for the prevention and suppression of potential threats.

COUNTERINTELLIGENCE PROTECTION OF CI

The Role of Counterintelligence Services in Protecting CI

In order to ensure adequate protection of CI, preventive action is essential, with security services playing a pivotal role in countering all forms of threats to national security and the safety of citizens. However, although security services constitute the primary actors in combating such threats, the preventive efforts of other stakeholders must not be neglected. These include education, cooperation with experts and the academic community, responsible media reporting, engagement of social and other public services in implementing a comprehensive platform to counter terrorism and other security threats (Babić, 2023: 220), as well as the promotion of dialogue and collaboration between governmental agencies and security professionals (Simeunović, 2009). Furthermore, success in countering the subversive activities of foreign entities or individuals and extremist and terrorist groups targeting CI necessitates robust international cooperation between security agencies and the intelligence communities of partner states (Babić, 2023).

The protection of CI is a fundamental priority of national security for any state, with counterintelligence services playing a crucial role in identifying, analysing and neutralising threats that may compromise its integrity. These services operate through preventive strategies, proactive threat identification and coordination with other security institutions to ensure that CI is maximally resilient to potential attacks.

The role of counterintelligence services can be observed through the following dimensions:

- *Intelligence collection and analysis*. Identifying potential threats through informational sources, technical surveillance and cooperation with partners (Clarke & Knake, 2019).
- *Detection and suppression of internal threats*. Implementing counterintelligence measures to prevent infiltration by hostile agents, sabotage and other forms of subversive activity (Office of the Director of National Intelligence, 2024).
- *Cooperation with CI sectors*. Integrating security measures through the exchange of information between public and private sectors to strengthen resilience (Cybersecurity and Infrastructure Security Agency [CISA], 2025).

In the Republic of Serbia, counterintelligence protection measures form part of the broader framework of security operations related to the protection of certain persons and facilities, both domestically and abroad. These tasks are directly carried out by the Ministry of the Interior, the Security Information Agency, the Military Security Agency, the Military Police and units of the Serbian Armed Forces (Article 1 of the Regulation on Determining Security Protection Tasks for Certain Persons and Facilities) (Uredba o određivanju poslova bezbednosne zaštite određenih lica i objekata, 2013).

Methods of Counterintelligence Protection of CI

Counterintelligence services apply a multilayered approach to the protection of critical infrastructure, relying on the synergy of technological, organisational and legal mechanisms. These methods are designed to enable the prevention, detection and neutralisation

of potential threats that could endanger the state's vital resources. Key counterintelligence protection strategies for CI include:

– Cyber security and advanced technological protection measures. Cyberspace represents one of the most vulnerable points in CI protection, due to the increasing frequency and sophistication of cyber attacks. Modern protection methods include the use of artificial intelligence to identify anomalies in network traffic, early detection of malicious software and swift incident response in order to minimise potential damage (Rid, 2020).
– The human factor represents one of the weakest links in the CI protection system. For this reason, counterintelligence measures include rigorous selection procedures and periodic security vetting of personnel who have access to sensitive data and strategically important facilities. These measures involve thorough background checks, financial analyses, psychological testing and the use of polygraph examinations to determine the reliability of candidates. Special emphasis is placed on the continuous monitoring of employees to identify potential security risks, such as susceptibility to corruption, presence of foreign influence, or inexplicable financial flows (Lowenthal, 2020).
– The counterintelligence apparatus conducts specialised operational activities aimed at identifying, tracking and neutralising hostile actors who seek to compromise critical infrastructure. These activities include surveillance of suspicious individuals and organisations, the application of covert data collection methods and the use of counter-disinformation techniques to neutralise potential threats. Particular importance is attached to activities targeting the detection of internal threats, where certain employees may become targets of foreign intelligence services or criminal organisations. Operational mechanisms of counterintelligence services also include simulated attacks, vulnerability analysis and the development of scenarios for timely responses in the event of crisis situations (U.S. Department of Homeland Security, 2020).

Challenges in Implementing Counterintelligence Measures

The implementation of counterintelligence measures in the modern security environment entails numerous complex challenges that require a multidisciplinary approach and continuous adaptation of institutional capacities. These challenges include:

– *Legal and ethical dilemmas*. The conduct of counterintelligence activities must be aligned with the principles of the rule of law and the protection of human rights and fundamental freedoms.
– *Rapid evolution of threats*. Contemporary security threats are characterised by a high degree of dynamism, with methods, tactics and technologies used by potential actors constantly evolving.
– *International cooperation*. In the context of global security threats, effective counterintelligence protection requires intensive cooperation among national and international actors. However, differing legal systems, political interests and levels of trust between states can present serious obstacles to information sharing. The develop-

ment of institutional mechanisms for coordination and harmonisation of procedures between partner countries, as well as with the private sector, becomes crucial to enhancing the security framework of CI (Clapper, 2018).

LEGAL AND INSTITUTIONAL FRAMEWORK FOR THE PROTECTION OF CI

The protection of CI relies on a legal and institutional framework that defines obligations, responsibilities and measures for preventing and responding to threats. This framework encompasses national laws, international standards and institutional structures that coordinate protection activities.

National Legal Framework

In the Republic of Serbia, the protection of CI is regulated by a series of legal acts that provide the basis for identifying, assessing risks, and implementing protective measures. Core documents include the Defence Act (Zakon o odbrani, 2018), the Defence Strategy (Strategija odbrane, 2019), the Critical Infrastructure Act (Zakon o kritičnoj infrastrukturi, 2018) and the National Security Strategy of the Republic of Serbia (Strategija nacionalne bezbednosti Republike Srbije, 2019). These acts define the obligations of CI entities, modes of cooperation between institutions and sectors, as well as crisis management procedures (Zakon o smanjenju rizika od katastrofa i upravljanju vanrednim situacijama, 2018; Uputstvo o metodologiji izrade i sadržaju procene rizika od katastrofa i plana zaštite i spasavanja, 2019).

Additionally, Law on Information Security from 2025 (Zakon o informacionoj bezbednosti, 2025) provides a regulatory framework for the protection of information and communication technology (ICT) systems within critical infrastructure, including obligations of ICT system operators and oversight of the implementation of cyber security measures.

Furthermore, the Strategy for the Development of the Information Society and Information Security for the period 2021–2026 highlights the need to maintain ICT systems of particular importance, i.e. critical information infrastructure and to ensure their uninterrupted functioning (Strategija razvoja informacionog društva i informacione bezbednosti za period od 2021. do 2026. godine, 2021).

Specifically, the Defence Strategy from 2019 states that the protection of the security of the Republic of Serbia and its citizens is also realised through the safeguarding of CI facilities, and that all preventive measures are to be undertaken accordingly. It further notes the need to establish an integrated information system for the security monitoring of CI facilities (Strategija odbrane, 2019).

Moreover, the current National Security Strategy from December 2019 emphasises that due to the growing number of conflicts caused by competition over energy resources, it is necessary to enhance the protection of critical energy infrastructure. The strategy also highlights that "critical infrastrucutre facilities will be identified and protected, and measures of early warning and preventive response will be implemented from the perspective

of protection against natural disasters, technical-technological accidents and catastrophes" (Strategija nacionalne bezbednosti Republike Srbije, 2019).

The Defence Act (Article 67) specifies that facilities of particular importance for national defence include: large technical-technological systems, facilities used for the production, storage or safeguarding of goods or services for defence purposes, facilities housing state authorities and legal entities of particular significance for national defence, as well as certain infrastructure facilities (Zakon o odbrani, 2018).

These strategic documents establish the priorities, methods and tools for maintaining the security of critical infrastructure. They also foresee interdepartmental cooperation, the development of crisis management capacities and the application of security standards based on best international practices.

International Standards and Regulations

The Organisation for Security and Co-operation in Europe (OSCE) also addresses issues related to the protection of CI and cyber security through its efforts to combat terrorism and cybercrime. In this context, participating States adopted in 2013 the first package of Confidence Building Measures (CBMs) aimed at reducing the risk of conflict arising from the use of information and communication technologies. The package was supplemented in 2016. In addition to more clearly defined principles for data exchange, the new guidelines directly call on member states to promote and improve mechanisms for public-private partnership in order to respond jointly to threats. Furthermore, the penultimate guideline refers to critical information infrastructure, upon which the functioning of CI depends, offering several models of cooperation in this field (Organization for Security and Co-operation in Europe, 2016).

Additionally, NATO's concept for the protection of key resources includes cooperation with the civil sector and private companies in order to enhance infrastructure resilience (North Atlantic Treaty Organization, 2024).

At the international level, European Union Agency for Cybersecurity (ENISA) provides technical support and strategic guidance for the protection of CI in the field of cyber security, while Interpol and Europol cooperate in suppressing criminal and terrorist threats directed at CI (United Nation Security Council, 2017).

In accordance with the above, Serbia is among the group of countries that recognise the global nature of terrorism and extremism in the context of potential threats to CI. Serbia advocates the need for continuous and extensive cooperation at both the global and regional level to establish a common approach, which is primarily realised through multilateral cooperation via the United Nations and other international organisations. As a candidate for European Union membership, Serbia strives to make a full contribution through active participation in European policy in the fight against terrorism, while respecting internationally recognised principles and standards (Živaljević, 2022: 209).

Institutional Actors and Their Responsibilities

At the national level, the responsibility for the protection of CI is shared among various institutions. In addition to the Ministry of the Interior, which is responsible for coordinating CI protection, the security services (the Security Intelligence Agency, the Military Security Agency and the Military Intelligence Agency) play a crucial role in the timely identification of intent and the prevention of plans that may, among other things, pose a threat to CI. The primary task of the security services is to safeguard vital national interests and values from security challenges, risks and threats. When it comes to the protection of Serbia's CI, the role of the security services is primarily reflected in the conduct of counterintelligence activities. This entails a "planned, organised, covert and continuous offensive-defensive operational engagement by a state's security services, primarily on its own territory, with the aim of detecting, monitoring, intercepting and preventing the activities of foreign intelligence services, individuals, groups and organisations on the territory of the home state that are directed against national security. Security services fulfil this task through high-quality assessment of the intentions and plans of external enemies, and by timely detection, effective monitoring, and either independently or in cooperation with other state and social actors, disabling foreign entities from uncovering vital and other confidential information of the home country" (Lakićević, 2022: 129).

Furthermore, the Defence Act (Zakon o odbrani, 2018) and the Armed Forces Act (Zakon o Vojsci Srbije, 2025) regulate issues concerning the protection of CI under the jurisdiction of the Ministry of Defence and the Serbian Armed Forces. Military and non-military challenges, risks and threats to national security, defined in Article 4 of the Defence Act, may undoubtedly endanger critical infrastructure, which necessitates the alignment of protection activities with the priority interests of the Republic of Serbia (Zakon o odbrani, 2018).

In addition to state institutions, the private sector also bears a degree of responsibility. Operators of CI in the fields of electricity, telecommunications and others, are obligated to implement internal security protocols and cooperate with relevant institutions. For instance, due to the sensitivity of the data accessible to individuals in the private sector, it is necessary to possess a security clearance certificate, preceded by a security vetting procedure for the respective legal or natural person (Zakon o tajnosti podataka, 2009).

CHALLENGES AND EXAMPLES OF GOOD PRACTICE

Although the legal and institutional framework for CI protection in Serbia is well developed, certain challenges hinder its effective implementation. These include insufficient coordination among state bodies, lack of financial resources and the ongoing need for technological advancement. Moreover, global trends in cyber security demand constant adjustment of the legal framework to address emerging threats.

States must ensure that the legislative framework remains flexible and adaptable to contemporary challenges, including hybrid threats and environmental sabotage. The implementation of internationally recognised standards and protection mechanisms is key to the long-term security of CI and the maintenance of the stability of systems that are vital to society.

Coordination Issues and Technological Challenges

The protection of CI requires a high level of coordination among different institutions and sectors, including governmental bodies, the private sector and international partners. One of the key issues is the insufficient exchange of information among entities responsible for security, which can lead to delays in threat response. Additionally, technological challenges, such as vulnerabilities in information systems and the growing complexity of hybrid threats, further complicate the protection of critical facilities and systems (Clarke & Knake, 2019).

The lack of integration of early warning systems and various security protocols within the national framework also adds to the challenges of CI protection. This problem is particularly pronounced in the energy and transport sectors, where digitalisation and system interdependence have increased the risk of cyber-attacks and sabotage (Lewis, 2018).

One of the key proposals for improvement is the harmonisation of national legislation with European standards, as well as the strengthening of public-private partnerships in the field of CI security. Moreover, it is necessary to enhance system resilience through regular security audits, capacity building for cyber defence and improved coordination among relevant actors. In addition to this, the development of a system for regular security assessments and infrastructure resilience testing through crisis simulation exercises is essential.

Examples from Practice and Successful Protection Models

The analysis of the existing protection models can provide useful guidance for improving security policies. The phrases "critical infrastructure" and "critical infrastructure protection" were first introduced in directives issued by the President of the United States. Specifically, the Homeland Security Act of 2002 provided for the establishment of the Department of Homeland Security (DHS). The Department is entrusted with all activities related to the protection of CI at the national level. Furthermore, within the framework of DHS, the Cyber and Infrastructure Security Agency (CISA) was established, serving as the coordinating authority for all identified sectors of CI (Ninković, 2021). In the United States, CISA has implemented a systematic approach to CI protection by integrating public and private sectors, with particular emphasis on continuous resilience testing (CISA, 2025). It is also important to highlight the National Strategy to Secure Cyberspace, which functions as an implementation component of the National Strategy for Homeland Security and is supplemented by the National Strategy for the Physical Protection of Critical Infrastructure and Key Assets. Securing cyberspace represents a complex strategic challenge requiring coordinated and focused efforts from society as a whole – including the federal government, state and local authorities, the private sector, and the American public. The strategic objectives of the National Strategy to Secure Cyberspace are as follows: preventing cyber attacks against America's critical infrastructure; reducing national vulnerabilities to cyber attacks; and minimizing damage and recovery time from cyber incidents that may occur (CISA, 2003).

The European Union, through Directive (EU) 2022/2557, has established more robust coordination mechanisms and clearer responsibilities for member states regarding the

identification and protection of CI, particularly in the energy and transport sectors (Directive (EU) 2022/2557 on the Resilience of Critical Entities, repealing Council Directive 2008/114/EC). These models may serve as a foundation for enhancing national strategies, including those in Serbia.

In Serbia, the National Security Strategy of 2019 provides for the improvement of both legal and operational frameworks in line with international standards, with particular emphasis on cooperation with international partners and the exchange of relevant data. This document highlights the importance of a proactive approach and the development of comprehensive protection models across all CI sectors (Strategija nacionalne bezbednosti Republike Srbije, 2019).

CONCLUSION AND RECOMMENDATIONS

In light of the topic discussed, this paper has sought to identify and analyse the complex security challenges increasingly faced by CI, particularly in the context of eco-terrorism and cyber operations. Emphasis has been placed on the necessity of linking counterintelligence and security approaches for the effective protection of vital systems, with particular attention to the transnational, technological and normative dimensions of such protection.

The analysis of CI vulnerabilities has shown that the security architecture of modern states is increasingly confronted with multi-vector threats, primarily those arising from cyberspace and hybrid forms of activity. Incidents such as attacks on power grids, industrial control systems and telecommunications resources highlight the profound vulnerability of vital systems and the urgent need to develop sustainable resilience mechanisms at a comprehensive level. Moreover, modern threats require more than technological solutions; they demand functional coordination, institutional synergy and interoperability between the public and private sectors, as well as transnational cooperation.

A particularly important insight of this paper is the emphasis on the specificity of cyber-attacks and eco-terrorism as forms of destructive activity directed against CI, distinguishing this phenomenon as a crucial focal point of counterintelligence and security analysis in the 21st century.

Internal challenges, such as normative inconsistencies, institutional fragmentation and limited technological resources, further complicate the establishment of an integrated CI protection system. International practice, particularly within the EU and the United States, highlights the importance of timely intelligence sharing, joint risk management and strategic planning based on assessments of long-term defence capacities.

Based on the analysis of challenges and best practice models, the following key recommendations can be identified for improving the CI protection system in the Republic of Serbia:

1) *Strengthening the legal framework.* It is essential to systematically enhance and harmonise the normative acts that define CI, its management and protection mechanisms, relying on the experiences of the EU member states and relevant international standards.
2) *Establishing operational coordination.* The introduction of clearly defined communication channels and protocols among stakeholders responsible for CI protection, in-

cluding ministries, regulatory bodies, infrastructure operators and security services, is vital for a swift and effective incident response.

3) *Developing cyber resilience capacities.* Investments in sophisticated tools for cyber-attack defence, expert education and the implementation of realistic attack simulations must become a systematic part of national strategy.
4) *Intensifying international cooperation.* It is necessary to deepen collaboration with partner states and services, as well as with international organisations, to align measures and undertake joint action in countering hybrid threats.
5) *Enhancing security culture.* Raising awareness among decision-makers, CI operators and the general public about the importance and vulnerability of CI is a prerequisite for building a sustainable and inclusive protection system.

CI forms the foundation of the functioning of modern society, and its protection should be positioned as a key component of national and global security. Contemporary trends of digitalisation, globalisation and increased interdependence of systems require the improvement of approaches through interdisciplinary cooperation, strategic planning and institutional innovation. In this regard, the contribution of this paper lies in its interdisciplinary examination of CI as a target of eco-terrorist and cyber-attacks, with particular emphasis placed on the counterintelligence and security aspects as strategic frameworks of defence. Past experiences clearly indicate that only holistically and proactively organised security systems can effectively respond to the challenges threatening the stability, sovereignty and security of a state in the 21st century.

REFERENCES

Babić, U. (2023). Preventivne mere u borbi protiv terorizma. *Megatrend revija, 20*(1), 219–230. https://doi.org/10.5937/MegRev2301219B

Barasa, E., Mbau, R., & Gilson, L. (2018). What is resilience and how it can be nurtured? A systematic review of empirical literature on organizational resilience. *International Journal of Health Policy and Management, 7*(6), 491–503. https://doi.org/10.15171/IJHPM.2018.06

Chalecki, E. L. (2002). A new vigilance: Identifying and reducing the risks of environmental terrorism. *Political Science Faculty Publications, 2(1), 46–64.* https://doi.org/10.1162/152638002317261463

Chalecki, E. L. (2024). Environmental terrorism twenty years on. *Global Environmental Politics* (2024), *24*(1), 1–9. https://doi.org/10.1162/glep_a_00728

Clapper, J. (2018). *Facts and fears: Hard truths from a life in intelligence*. Viking Press.

Clarke, R. A., & Knake, R. K. (2019). *The fifth domain: Defending our country, our companies, and ourselves in the age of cyber threats*. Penguin Press.

Cybersecurity and Infrastructure Security Agency (CISA). (2003). *The National Strategy to Secure Cyberspace*. https://www.cisa.gov/sites/default/files/publications/cyberspace_strategy.pdf

Cybersecurity and Infrastructure Security Agency (CISA). (2025). *Partnerships and collaboration*. https://www.cisa.gov/topics/partnerships-and-collaboration.

Directive (EU) 2022/2557. *On the resilience of critical entities, repealing Council Directive 2008/114/EC*. European Parliament and Council. https://eur-lex.europa.eu/eli/dir/2022/2557/oj/eng

Directive (EU) 2024/1203. *On the protection of the environment through criminal law and replacing directives 2008/99/EC and 2009/123/EC*. European Parliament and Council. https://eur-lex.europa.eu/eli/dir/2024/1203/oj/eng

Domović, R. (2017). Cyber-attacks as a threat to critical infrastructure. *International Conference the Future of Information Sciences, INFuture2017: Integrating ICT in Society*, *6*, 259–269. https://doi.org/10.17234/INFUTURE.2017.26

Costa, R. (2021). *Hybrid threats in the context of European security* [Report]. International conference organized at the National Defence Institute (IDN), Lisbon, Portugal. Instituto da Defesa Nacional. https://www.idn.gov.pt/pt/publicacoes/ebriefing/Documents/E-Briefing%20Papers/E-Briefing%20Papers%203.pdf

Geers, K. (2009). The cyber threat to national critical infrastructures: Beyond theory. *Information Security Journal: A Global Perspective*, *18*(1), 1–7. https://doi.org/10.1080/19393550802676097

Jovanović, L. (2025, July 1). Top 10 najvećih hakerskih napada u istoriji: Kako su promenili svet. *Web Mind*. https://web-mind.rs/sajber-bezbednost/top-10-najvecih-hakerskih-napada-u-istoriji-kako-su-promenili-svet/

Lakićević, M. (2022). Kontraobaveštajna delatnost u cilju suzbijanja organizovanog kriminala. *Nacionalni interes*, *43*(1), 123–145. https://doi.org/10.22182/ni.4312022.6

Lewis, J. A. (2018). *Rethinking cybersecurity: Strategy, mass effect, and states.* Center for Strategic & International Studies.

Lowenthal, M. (2020). *Intelligence: From secrets to policy*. SAGE Publications.

Nacionalni CERT Republike Srbije. (2022). *Godišnji izveštaj o stanju sajber bezbednosti u Republici Srbiji. www.cert.rs/files/shares/Izvestaj%20o%20statisti%C4%8Dkim%20podacima%20za%202022.%20godinu.pdf*

National Infrastructure Advisory Council. (2009, September 8). *Critical infrastructure resilience: Final report and recommendations*. https://www.cisa.gov/sites/default/files/publications/niac-critical-infrastructure-resilience-final-report-09-08-09-508.pdf

Ninković, V. M. (2021). Critical infrastructure resilience: National approaches in the United States of America, the United Kingdom and Australia. *Zbornik radova Pravnog fakulteta, Novi Sad*, *55*(4), 1205–1225. https://doi.org/10.5937/zrpfns55-30333

North Atlantic Treaty Organization (NATO). (2024). *Resilience, civil preparedness and Article 3*. https://www.nato.int/cps/en/natohq/topics_132722.htm

Office of the Director of National Intelligence. (2024). *National counterintelligence strategy 2024*. National Counterintelligence and Security Center. https://www.dni.gov/files/NCSC/documents/features/NCSC_CI_Strategy-pages-20240730.pdf

Organization for Security and Co-operation in Europe (OSCE). (2016, March 10). *Decision no. 1202 OSCE, Confidence-building measures to reduce the risks of conflict stemming from the use of information and communication technologies*. Permanent Council. https://www.osce.org/files/f/documents/d/a/227281.pdf

Putnik, N. (2023). Metodologija izrade strategije nacionalne bezbednosti Republike Srbije – dileme i perspektive. In B. Banović, & N. Stekić (Eds.), *Strateški i normativni okvir Republike Srbije za reagovanje na savremene bezbednosne rizike* (pp. 21–36). Fakultet bezbednosti Univerziteta u Beogradu. https://newsimrdproject.fb.bg.ac.rs/rez/rez19.pdf

Rid, T. (2020). *Active measures: The secret history of disinformation and political warfare.* Farrar, Straus and Giroux.

SANS Institute. (2016, March 18). *Analysis of the cyberattack on the Ukrainian power grid*. https://nsarchive.gwu.edu/sites/default/files/documents/3891751/SANS-and-Electricity-Information-Sharing-and.pdf

Savolainen, J. (2019, November). *Hybrid CoE working paper 4: Hybrid threats and vulnerabilities of modern critical infrastructure – Weapons of mass disturbance (WMDi)?* The European Centre of Excellence for Countering Hybrid Threats. https://www.hybridcoe.fi/publications/hybrid-coe-working-paper-4-hybrid-threats-and-vulnerabilities-of-modern-critical-infrastructure-weapons-of-mass-disturbance-wmdi/

Simeunović, D. (2009). Serbian efforts in transportation security against terrorism. *The Review of International Affairs, 60*(1133–1134), 5–8.

Somers. S. (2019). *How terrorists leverage climate change*. New Security Beat. https://www.newsecuritybeat.org/2019/09/terrorists-leverage-climate-change/

Stojanović, Z., & Bodrožić, I. (2025). Possibilities and scope of environmental protection through criminal law: The new environmental crime directive. *NBP. Nauka, bezbednost, policija, 30*(1), 1–19. https://doi.org/10.5937/nabepo30-55088

Strategija nacionalne bezbednosti Republike Srbije [National Security Strategy of the Republic of Serbia]. (2019). *Službeni glasnik Republike Srbije*, 94/2019. https://pravno-informacioni-sistem.rs/eli/rep/sgrs/skupstina/strategija/2019/94/2

Strategija odbrane [Defence Strategy]. (2019). *Službeni glasnik Republike Srbije*, 94/2019. https://pravno-informacioni-sistem.rs/eli/rep/sgrs/skupstina/strategija/2019/94/1

Strategija razvoja informacionog društva i informacione bezbednosti za period od 2021. do 2026. godine [Strategy for the Development of the Information Society and Information Security for the period]. (2021). *Službeni glasnik Republike Srbije*, 86/2021. https://pravno-informacioni-sistem.rs/eli/rep/sgrs/vlada/strategija/2021/86/1/reg

United Nations Security Council. (2017). *Physical protection of critical infrastructure against terrorist attacks*. Counter-Terrorism Committee Executive Directorate. https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021/Jan/cted-trends-report-march-2017-final.pdf

United Nation Security Council. (2017, February 13). *Security Council resolution 2341 (2017) [on protection of critical infrastructure against terrorist acts]* (Resolution S/RES/2341(2017)). United Nations Digital Library. https://digitallibrary.un.org/record/859472?ln=en

Uputstvo o metodologiji izrade i sadržaju procene rizika od katastrofa i plana zaštite i spasavanja [Instruction on the Methodology for Risk Assessment and the Content of the Protection and Rescue Plan]. (2019). *Službeni glasnik Republike Srbije*, 80/2019.

Uredba o određivanju poslova bezbednosne zaštite određenih lica i objekata [Regulation on Determining Security Protection Tasks for Certain Persons and Facilities], *Službeni glasnik Republike Srbije*, 72/2010, 64/2013. https://pravno-informacioni-sistem.rs/eli/rep/sgrs/vlada/uredba/2010/72/4

U.S. Department of Homeland Security. (2020). *DHS counterintelligence program*. https://www.dhs.gov/sites/default/files/publications/privacy-pia-dhsall086-ciprograms-august2020.pdf

Venkatachary, S. K., Prasad, J., Alagappan, A., Andrews, L. J. B., Raymon, R. A., & Duraisam S. (2024). Cybersecurity and cyber-terrorism challenges to energy-related infrastructures – Cybersecurity frameworks and economics: Comprehensive review. *International Journal of Critical Infrastructure Protection*, *45*, 100677. https://doi.org/10.1016/j.ijcip.2024.100677

Zakon o informacionoj bezbednosti [Law on Information Security]. (2025). *Službeni glasnik Republike Srbije*, 91/2025. https://pravno-informacioni-sistem.rs/eli/rep/sgrs/skupstina/zakon/2025/91/5/reg%20

Zakon o kritičnoj infrastrukturi [Critical Infrastructure Act]. (2018). *Službeni glasnik Republike Srbije*, 87/2018. https://pravno-informacioni-sistem.rs/eli/rep/sgrs/skupstina/zakon/2018/87/8

Zakon o odbrani [Defence Act]. (2018). *Službeni glasnik Republike Srbije*, 36/2018. https://www.paragraf.rs/propisi/zakon_o_odbrani.html

Zakon o smanjenju rizika od katastrofa i upravljanju vanrednim situacijama [Law on Disaster Risk Reduction and Emergency Management]. (2018). *Službeni glasnik Republike Srbije*, 87/2018. https://www.paragraf.rs/propisi/zakon-o-smanjenju-rizika-od-katastrofa-i-upravljanju-vanrednim-situacijama.html

Zakon o tajnosti podataka [Classified Information Act]. (2009). *Službeni glasnik Republike Srbije*, 104/2009. https://pravno-informacioni-sistem.rs/eli/rep/sgrs/skupstina/zakon/2009/104/7

Zakon o Vojsci Srbije [Law on the Serbian Armed Forces]. (2025). *Službeni glasnik Republike Srbije*, 109/2025. https://pravno-informacioni-sistem.rs/eli/rep/sgrs/skupstina/zakon/2007/116/2/reg

Živaljević, D. (2022). *Radikalizacija društva i terorizam.* Akademija za nacionalnu bezbednost/Službeni glasnik.