International Scientific Conference 20 UNITECH 26

INTERNATIONAL SCIENTIFIC CONFERENCE
19-21 November 2026
GABROVO

RESILIENCE ANALYSIS OF THE CRITICAL ICT INFRASTRUCTURE OF THE CITY OF DOBOJ IN THE CONTEXT OF ICT HYBRID AND TERRORIST THREATS

Sandi Božičković [1], Branislav Božičković [2], Ratko Garić [3]

[1] *Comunication and Electro-engineering School, Cara Dušana 18, Doboj, Bosnia and Herzegovina*
[2] *Court interpreeter, Nikole Pašića 1L/9, Doboj, Bosnia and Herzegovina*
[3] *College of Professional Studies for Management and Business Communications, Belgrade, Serbia*

……
**Corresponding author: sandi.bozickovic@gmail.com*

Abstract
This paper investigates the vulnerability of information and communication technology (ICT) in the area of the city of Doboj, with a special focus on the power sector and crisis management systems. Doboj, as a key transport and energy hub of the Republika Srpska, represents a high-priority target for potential terrorist acts combining physical sabotage and cyber-attacks. The paper analyzes the current protection systems, identifies critical points in the "Elektrodoboj" network, and proposes a model for improving resilience through network segmentation and the establishment of a local incident response center.

Keywords: Critical infrastructure, Doboj, Cyber-terrorism, Power grid, ICT security..

INTRODUCTION

The city of Doboj represents one of the most important strategic points of the Republika Srpska. Its importance stems not only from its administrative role, but also from the fact that Doboj is the main communication and infrastructure hub connecting the western and eastern parts of the Republika Srpska, as well as key corridors towards the Federation of Bosnia and Herzegovina and, more broadly, towards the European Union. Doboj is located at the confluence of the Spreča River into Bosnia, at the point where major railway routes and road corridors (Corridor Vc) intersect. In ICT terms, the backbone of the optical network of the Republika Srpska passes through Doboj. Any disruption in this hub has immediate consequences on:

Energy stability: The "Elektro-Doboj Electrical Utility company" hubs are crucial for the distribution of electricity to the north and west.

Telecommunications traffic: The outage of local routers and base stations isolates large parts of the Posavina and Krajina regions.

A particular challenge for information and communication security is the close proximity of the inter-entity boundary line. The city of Doboj borders several municipalities in the Federation of Bosnia and Herzegovina (Tešanj, Maglaj, Gračanica, Usora). This administrative and territorial intertwining in crisis situations can lead to:

- Jurisdictional barriers: The problem of rapid coordination between police agencies (RS MoI and cantonal MoIs) during a cyber-terrorist attack.

This is an open access article licensed under Creative Commons Attribution 4.0 International
Print ISSN: 1313-230X, Online ISSN: 3033-1404

- Technical interference: Frequency overlap and dependence on shared telecommunications resources located in peripheral areas.

The City of Doboj represents an important case for critical infrastructure resilience analysis due to its strategic geographical position and its role as a major transport, energy, and communication hub in Bosnia and Herzegovina. Important road and railway corridors, telecommunications networks, energy infrastructure, and public services are concentrated in this area, increasing both its strategic importance and its exposure to cyber, hybrid, and physical threats. The strong interdependence between these systems further increases the potential consequences of infrastructure disruption [1].

DEFINING CRITICAL ICT INFRASTRUCTURE AT THE LOCAL LEVEL

In the modern urban environment, the concept of infrastructure is no longer limited to roads, bridges and the power grid. Critical ICT infrastructure (KII) is a digital foundation whose disruption, due to a deliberate attack or technical failure, would lead to a serious threat to the security, economy and health of citizens at the local level. At the level of local government such as Doboj, critical ICT infrastructure is classified into three interdependent domains[2]:

1. **Public resource management systems (SCADA and IoT):** Systems that enable automated management of water supply (pumps, tanks), thermal energy and traffic regulation. These systems are most vulnerable to terrorist acts aimed at physical and cyber sabotage.
2. **Communication and network core:** Optical network connecting institutions, mobile phone base stations and internet hubs.
3. **Transport control ICT:** Doboj, as a railway and road junction, also has a specific ICT infrastructure intended for transport control, which is of strategic importance for the region.

Unlike national infrastructure, the local ICT infrastructure in Doboj has specific characteristics:

- **High degree of correlation with physical security:** The collapse of network systems directly disables the operation of video surveillance of public areas and communication of emergency services (police, firefighters).
- **Limited redundancy:** Local systems often do not have backup locations (disaster recovery centers) at a sufficient geographical distance, which makes them vulnerable to localized terrorist attacks or natural disasters.
- **Interdependence:** Digital infrastructure is a "system of all systems." Its failure causes cascading effects – for example, the inability to make electronic payments leads to disruptions in the supply of essential food and fuel in crisis situations [3].

GEOSTRATEGIC POSITION OF THE CITY OF DOBOJ

Doboj occupies a central position in the northern part of Bosnia and Herzegovina (Republika Srpska) and represents one of the most important transport and communication hubs in the region. Its geostrategic importance is directly reflected in the vulnerability of ICT systems through the following aspects [4]:

- **Hub of Pan-European Corridors:** The city is located at the intersection of key road and rail routes, primarily Corridor Vc and main routes connecting the western and eastern parts of Republika Srpska. Primary

optical infrastructure is laid along these transport corridors. Any interruption causes a "blackout" or significant slowdown of digital traffic on a wider regional level.

- **Regional logistics and energy center:** Disabling ICT systems that manage logistics in Doboj could paralyze the movement of goods and energy, going beyond local significance to become an entity or state security problem.
- **Administrative and multiethnic position:** Located on the administrative line between entities, Doboj experiences high frequency of people, capital, and information. Such environments are fertile ground for information operations and the spread of disinformation.
- **Hydrographic factor and natural disasters:** Location on three rivers (Bosna, Spreča, Usora) makes Doboj susceptible to natural disasters (such as the floods of 2014) [5]. Without stable communication links, effective response to a hybrid threat during a natural disaster is impossible.

The geostrategic position of Doboj transforms it into a "single point of failure" in the region's communications network. Protecting its ICT infrastructure from hybrid and terrorist threats is an imperative for regional stability [4].

Level	Function of ICT infrastructure in Doboj	Security priority
Local (Doboj)	Operation of city services, water supply, heating plant	Continuity of essential services
Regional (RS)	Connecting east and west of RS, railway management	Stability of transport and communications
State (BiH)	Transit of data to the EU, control of the Vc corridor	International reputation and information flow

Fig. 1. *Strategic importance of the Doboj hub in relation to levels of government*

HYBRID AND TERRORIST THREATS

Threats to critical ICT infrastructure can be divided into three basic categories: cyberterrorism/digital sabotage, hybrid threats/information operations, and physical attacks with ICT consequences [6]:

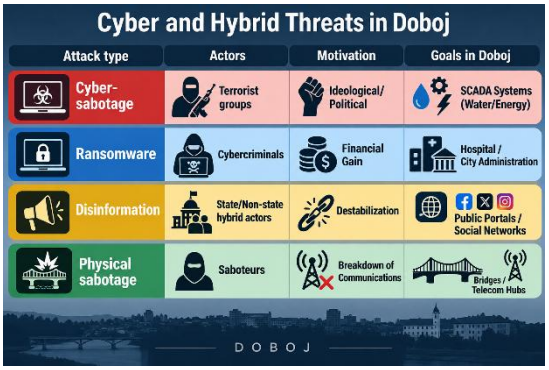


Fig. 2. *Threat matrix according to actors and motivation*

- **Cyberterrorism and digital sabotage:** Includes ransomware attacks (e.g., encrypting hospital or city administration data), Distributed Denial of Service (DDoS) flooding emergency services, and Advanced Persistent Threats (APT) targetting SCADA systems.
- **Hybrid threats and information operations:** Uses ICT infrastructure for society manipulation, fake news dissemination during crises, and phishing attacks on public employees.
- **Physical attacks with ICT consequences:** Sabotage of fiber optic cables over key bridges (Bosna, Spreča, Usora) or power grid attacks causing blackouts [7].

RESEARCH METHODOLOGY

This paper applies a combined methodological approach integrating qualitative and quantitative research methods, with an emphasis on a case study for the territory of the City of Doboj. The research utilized the following scientific methods:

- **Analysis and Synthesis Method:** Used to decompose the complex critical infrastructure system into its constituent components (energy sector, telecommunications, public administration, healthcare, and transport), as well as to synthesize data on interdependencies and cascading effects during disruptions.
- **Structural-Functional Method:** Applied to examine the role and importance of Doboj as a key geostrategic, transport, and telecommunications transit hub at the level of Republika Srpska and Bosnia and Herzegovina.
- **Risk and Threat Assessment Method:** Utilized to analyze threat matrices (hybrid threats, cyber-terrorism, and physical sabotage) and define vulnerability levels of local ICT systems (such as SCADA systems and electrical power hubs).
- **Comparative Analysis and Normative-Legal Method:** Relevant legal frameworks, European Union directives (such as Directive 2008/114/EC), and the Republika Srpska Law on Critical Infrastructure Security were analyzed to identify regulatory and jurisdictional barriers along inter-entity boundary lines.

Primary and secondary sources included spatial data from the Republic Administration for Geodetic and Property Affairs of Republika Srpska (RUGIP), strategic studies, as well as domestic and international scientific literature in the fields of cybersecurity and critical infrastructure protection.

RESEARCH HYPOTHESES

Starting from the research problem concerning ICT infrastructure vulnerability under modern hybrid and terrorist threats, the paper establishes one general and two specific hypotheses:

- **General Hypothesis (H0):** The high concentration of transport, energy, and telecommunications functions in the City of Doboj, lacking adequate geographic redundancy and network segmentation, renders its local ICT infrastructure a "Single Point of Failure" whose compromise would trigger a cascading collapse of vital municipal and regional services.
- **Specific Hypothesis 1 (H1):** Hybrid threats, combined with cyber-terrorism and physical sabotage of key hubs (such as power substations and optical routes across river bridges), represent a dominant security challenge directly threatening the continuity of electricity supply and crisis management operations.
- **Specific Hypothesis 2 (H2):** The proximity of the inter-entity boundary line and specific administrative-territorial interactions complicate rapid coordination among competent agencies, necessitating the immediate establishment of a local incident response center and decentralized protection systems.

PURPOSE OF THE STUDY

The primary purpose of the study is to investigate the vulnerabilities of the information and communication technology (ICT) infrastructure within the City of Doboj—focusing specifically on the power sector and crisis management systems—to understand how potential hybrid and terrorist threats can trigger cascading disruptions across regional energy, transport, and communication networks. To fulfill this purpose, the paper outlines the following key objectives:

- Identify Strategic Vulnerabilities: Analyze Doboj's unique geostrategic position as a primary transport,

energy, and telecommunications transit hub (connecting western and eastern Republika Srpska, entities, and European corridors) to understand its susceptibility to single-point-of-failure disruptions.

- Classify Critical Local ICT Domains: Define and categorize local critical ICT infrastructure into interdependent domains, including public resource management (SCADA and IoT), communication/network cores, and transport control systems.
- Evaluate Threat Scenarios: Examine modern security risks through a threat matrix encompassing cyberterrorism/digital sabotage (such as ransomware, DDoS, and APTs), hybrid operations (disinformation and social engineering), and physical attacks combined with ICT consequences (such as fiber optic sabotage and power grid blackouts) [8].

Propose Resilience-Enhancing Models: Formulate strategic and technical recommendations to improve local and regional security, including developing decentralized and redundant systems, improving ICT/energy network protection, integrating smart monitoring technologies, and establishing local incident response mechanisms.

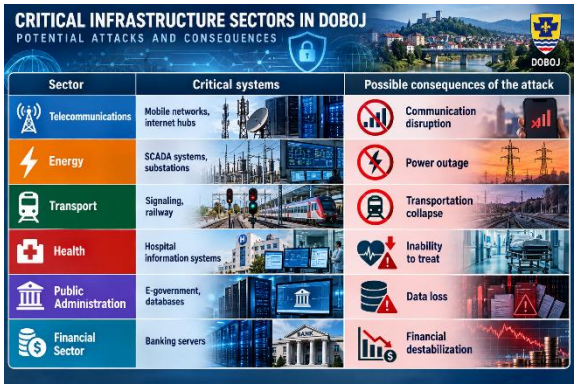


Fig. 3. *Key elements of critical ICT infrastructure*

CONCLUSION

The analysis of the critical infrastructure of the city of Doboj shows that this urban area has an extremely important strategic position, but at the same time a pronounced systemic vulnerability. As one of the key transport and logistics hubs in Bosnia and Herzegovina, Doboj functions as a central point connecting road and rail transport, energy flows and telecommunications networks. However, it is precisely this concentration of functions that increases the risk of a domino effect: an interruption in one sector – especially in energy or ICT infrastructure – can cause chain disruptions in traffic, water supply, health services and the work of public institutions. To increase the resilience of the city, it is necessary to:

- Develop decentralized and redundant systems;
- Improve the protection of ICT and energy networks;
- Integrate smart technologies for monitoring and management;
- Strengthen capacities for crisis management and rapid response;
- Plan infrastructure in accordance with climate risks.

In conclusion, the future security and functionality of the city of Doboj depends on the ability to view critical infrastructure as an interconnected system and to plan its protection in an integrated manner, through technical, organizational, and strategic measures.

RESULTS AND DISCUSSION

The analysis of Doboj's critical ICT infrastructure confirmed the initial hypotheses regarding its high level of systemic vulnerability

The study confirmed the general hypothesis (H0): due to the convergence of Pan-European Corridor Vc, railway junctions, and primary optical backbones (m:tel, BH Telecom, HT Eronet) in Doboj, the local infrastructure serves as a critical Single Point of Failure. Disruptions in these

hubs trigger cascading failures across regional power supplies and telecommunications throughout the wider Posavina and Krajina regions.

The analysis supports the first specific hypothesis (H1):

- **SCADA Systems and Energy:** Represent the sectors with the highest vulnerability and catastrophic potential consequences in the event of an attack.
- **Healthcare and Telecommunications:** Ransomware attacks targeting the "St. Apostol Luka" Hospital or DDoS attacks on emergency services severely threaten public health and crisis management.
- **Hybrid Operations:** Proximity to the inter-entity boundary line facilitates the spread of disinformation via local digital channels during crises.

The results validate the second specific hypothesis (H2): administrative-territorial intertwining and proximity to municipalities in the Federation of Bosnia and Herzegovina (Tešanj, Maglaj, Gračanica) slow down rapid coordination between police agencies and competent authorities (RS MoI and cantonal MoIs) during cyber-terrorist attacks. This highlights the urgent need to establish a local incident response center (CSIRT) and decentralized protection systems.

REFERENCE

[1] Republic Administration for Geodetic and Property Affairs of Republika Srpska Spatial data and infrastructure maps of Republika Srpska. Banja Luka: Republic Administration for Geodetic and Property Affairs, 2023.

[2] Đukić S. Detective activity – normative framework and practical approach. Banja Luka: Faculty of Security and Protection, 2021.

[3] Kovačević M, Petrović D. 'Critical infrastructure protection in Southeast Europe: Challenges and perspectives', Journal of Security Studies, 2021: 14(2), pp. 45–60.

[4] Stanić R. 'Izazovi sajber bezbjednosti u kritičnoj infrastrukturi Republike Srpske', Godišnjak Fakulteta bezbjednosnih nauka, 2021:3(1), pp. 112–128.

[5] Kerttunen M. Cyberwarfare and Resilience: National Tactics and Strategies. Helsinki: National Defence University, 2021.

[6] Peng Z, Yan C. and Xiaoli Li. 'Cybersecurity challenges in critical infrastructure systems', IEEE Access, 7, 2021, pp. 45306–45320. doi:10.1109/ACCESS.2019.2909828.

[7] Stojanović B.'Upravljanje rizicima u zaštiti kritične infrastrukture', Bezbednost, 2021: 62(3), pp. 89–102.

[8] Government of Republika Srpska. Law on the Security of Critical Infrastructures of the Republic of Srpska. Official Gazette of the Republic of Srpska, No. 58/19, 16 July 2019.