Conference Book Of Abstracts

4TH INTERNATIONAL CONFERENCE ON CRITICAL INFRASTRUCTURE

RESILIENCE OF THE CRITICAL INFRASTRUCTURE OF THE REPUBLIC OF SERBIA AT THE INTERSECTION OF GEOPOLITICS, ARTIFICIAL INTELLIGENCE AND CLIMATE CHANGE

5-6 November 2026, Hotel "Palisad", Zlatibor, Serbia



November, 2026

BOOK OF ABSTRACTS

The 4th International Conference on Critical Infrastructure:

RESILIENCE OF THE CRITICAL INFRASTRUCTURE OF THE REPUBLIC OF SERBIA AT THE INTERSECTION OF GEOPOLITICS, ARTIFICIAL INTELLIGENCE AND CLIMATE CHANGE
SKI 26



Republic of Serbia

MINISTRY OF SCIENCE,
TECHNOLOGICAL DEVELOPMENT AND INNOVATION

November 5–6, Zlatibor, Serbia

The 4th International Conference on Critical Infrastructure:

RESILIENCE OF THE CRITICAL INFRASTRUCTURE OF THE REPUBLIC OF SERBIA AT THE INTERSECTION OF GEOPOLITICS, ARTIFICIAL INTELLIGENCE AND CLIMATE CHANGE

SKI 26 – BOOK OF ABSTRACTS

Editors

Prof. dr Zoran Keković

Dr Marina Dabetić

Proofreader

Marko Ristić

Technical assistant

Marija Stanković

Publisher

Center for Risk Analysis and
Crisis Management

Press

Data Copy

Print run:

300 copies

ISBN 978-86-909840-0-8

Zlatibor, November 2026

Organizers

Center for Risk Analysis and Crisis Management

With the support of the Ministry of Science, Technological Development and Innovation of the Republic of Serbia

Co-organizers

Faculty of Security Studies, University of Belgrade

Institute for Standardization of Serbia

Institute of International Politics and Economics

Institute for Political Studies

Atlantic Council of Montenegro

Singidunum University

HUB201

Jaroslav Černi Water Institute

C O N T E N T

Preface 5

CHAPTER 1: GEOPOLITICS AND CRITICAL INFRASTRUCTURE RESILIENCE 7

SECURITY OF NUCLEAR POWER PLANTS UNDER THE SHADOW OF GEOPOLITICAL SHIFTS
Şebnem Udum, Department of International Relations, Hacettepe University, Ankara, Türkiye 8

SECURING THE INFRASTRUCTURE OF OTHERS? CHINA'S APPROACH TO CRITICAL INFRASTRUCTURE SECURITY AND ITS IMPLICATIONS FOR PARTNER STATES
Nenad Stekić, Faculty of Security Studies, University of Belgrade, Serbia 9

RESILIENCE OF THE REPUBLIC OF SERBIA'S TRANSPORT AND LOGISTICS INFRASTRUCTURE TO GEOPOLITICAL DISRUPTIONS
Nataša Stanojević, Institute of International Politics and Economics, Belgrade, Serbia
Gordana Mišev, Institute of International Politics and Economics, Belgrade, Serbia 10

STRATEGIC MARITIME CHOKEPOINTS AND ENERGY SECURITY: UPDATING MAHAN'S SEA POWER THEORY IN THE CONTEMPORARY GEOPOLITICAL CONTEXT
Jadranka Polović, Libertas International University, Zagreb, Croatia 11

THE CHALLENGES WITHIN CRITICAL INFRASTRUCTURE, AS A POTENTIAL FOR PRAGMATIC WESTERN BALKANS INTEGRATION ON THE EU PATH
Mitko Arnaudov, Institute of International Politics and Economics, Belgrade, Serbia
Sanja Jelisavac Trošić, Institute of International Politics and Economics, Belgrade, Serbia 13

ENERGY SOVEREIGNISM AND NATIONAL SECURITY
Nenad Šijaković, JSC Elektromreža Srbije, School of electrical engineering University of Belgrade
Branko Djordjević, JSC Elektromreža Srbije, School of electrical engineering University of Belgrade 14

DETERMINANTS OF THE PROFILES OF MIGRANTS IN TRANSIT THROUGH THE WESTERN BALKANS – CLUSTER ANALYSIS
Zoran Milosavljević, Institute for Political Studies, Serbia
Mirjana Landika, Pan-European University "Apeiron", Bosnia and Herzegovina 16

CHAPTER 2: ARTIFICIAL INTELLIGENCE AND DIGITAL TRANSFORMATION OF CRITICAL INFRASTRUCTURE 17

CRISIS DECISION-MAKING UNDER UNCERTAINTY: THE ROLE OF ARTIFICIAL INTELLIGENCE IN STRENGTHENING CRITICAL INFRASTRUCTURE RESILIENCE
Zoran Keković, Faculty of Security Studies, University of Belgrade, Serbia 18

METAHEURISTIC OPTIMIZATION OF ASYMMETRIC XGBOOST FOR INTERPRETABLE IOT AND INDUSTRIAL IOT INTRUSION DETECTION
Nebojša Bačanin Džakula, Singidunum University
Zoran Keković, Faculty of Security Studies, University of Belgrade, Serbia 19

CRISIS COMMUNICATION DURING CBRN INCIDENTS: SOCIAL MEDIA AND AI-GENERATED CONTENT
Marina Dabetić, "Vinča" Institute of Nuclear Sciences - National Institute of the Republic of Serbia, University of Belgrade, Serbia
Ema Kraktus, Ministry of Education, Serbia
Jadranka Miletić Vukajlović, "Vinča" Institute of Nuclear Sciences - National Institute of the Republic of Serbia, University of Belgrade, Serbia 20

FROM NORMS TO PRACTICE: PROTECTING CRITICAL INFRASTRUCTURE IN SERBIA IN THE AGE OF ARTIFICIAL INTELLIGENCE
Dragana Dabić, Institute of International Politics and Economics, Belgrade, Serbia
Jelica Gordanić, Institute of International Politics and Economics, Belgrade, Serbia
Ivana Dunjić, Institute of International Politics and Economics, Belgrade, Serbia 21

AI-ENABLED CYBERCRIME
Gil Baram, University of South Florida, Bellini College of AI, Cybersecurity and Computing, USA 22

AI ASSISTANTS IN WATER INFRASTRUCTURE MANAGEMENT: BOUNDARIES OF TRUST AND RESPONSIBILITY
Nikola Milivojević, Jaroslav Černi Water Institute, Belgrade, Serbia
Vladimir Milivojević, Jaroslav Černi Water Institute, Belgrade, Serbia
Ivana Krtolica, The Institute for Artificial Intelligence Research and Development of Serbia, Novi Sad, Serbia 23

RADIO FREQUENCY MONITORING FOR UAV DETECTION: A COMPARATIVE ANALYSIS OF TECHNOLOGIES AND CHALLENGES IN CRITICAL INFRASTRUCTURE PROTECTION
Inda Kreso, GEOPOL – Center for Geopolitical Research, Sarajevo, Bosnia and Herzegovina
Irma Sokolović, Woman4Cyber Bosnia and Herzegovina, Sarajevo, Bosnia and Herzegovina 24

READINESS OF PRIMARY SCHOOLS IN SERBIA TO RESPOND TO CRITICAL INFRASTRUCTURE BREAKDOWN AND EMERGENCY SITUATIONS: AN EMPIRICAL ANALYSIS OF OCCUPATIONAL SAFETY AND HUMAN CAPITAL PROTECTION SYSTEMS
Jelena Marković, Mozzart Foundation, Belgrade, Serbia 25

ARTIFICIAL INTELLIGENCE GOVERNANCE AND ALIGNMENT WITH ETHICAL PRINCIPLES IN HEALTHCARE
Lepa Babić, Singidunum University 26

CASE STUDY: AI, HUMAN DIGNITY AND GLOBAL RISKS
Bogdan Filipović, "Živko Ljujić" Primary School, Serbia 27

REGULATORY TRANSFORMATION OF CRITICAL INFRASTRUCTURE IN THE ERA OF ARTIFICIAL INTELLIGENCE: THE EUROPEAN FRAMEWORK AND THE PERSPECTIVE OF SERBIA
Ivana Vlašković, Institute for Political Studies, Belgrade, Serbia 28

CHAPTER 3: CLIMATE CHANGE, EXTREME EVENTS AND CRITICAL INFRASTRUCTURE RESILIENCE 29

ARTIFICIAL INTELLIGENCE, CLIMATE RISK AND CRITICAL INFRASTRUCTURE: ETHICAL ASPECTS OF RESPONSIBILITY AND HUMAN OVERSIGHT IN AUTOMATED DECISION-MAKING
Velimir Strugar, Directorate for IMS and General Affairs, Nikšić, Montenegro... 30

THE PARADIGM OF RESILIENCE AND CONTROLLED DEVELOPMENT OF THE ELECTRICAL POWER SYSTEM IN THE ERA OF CLIMATE EXTREMES AND HYBRID GEOPOLITICAL PRESSURES
Nenad Šijaković, JSC Elektromreža Srbije, School of electrical engineering University of Belgrade, Serbia
Branko Djordjević, JSC Elektromreža Srbije, School of electrical engineering University of Belgrade, Serbia
Branislav Djukić, Electricity Coordinating Center - EKC, Belgrade, Serbia 31

APPLICATION AND LIMITATIONS OF ARTIFICIAL INTELLIGENCE (AI) IN AVIATION SECURITY (AvSec)
Gjorgji Alceski, TAV Macedonia, Ohrid St. Paul the Apostle Airport, Ohrid, North Macedonia 32

BEYOND PROTECTION: THE EU'S 2026 GUIDELINES ON CRITICAL ENTITIES RESILIENCE
Sanja Grbović, Faculty of Law, University of Montenegro, Podgorica, Montenegro 33

CHAPTER 4: AN INTEGRATED APPROACH TO CRITICAL INFRASTRUCTURE RESILIENCE IN THE REPUBLIC OF SERBIA.....35

DYNAMIC ADAPTIVE CRISIS PLANNING: A CONCEPTUAL FRAMEWORK FOR CRISIS RESPONSE UNDER DEEP UNCERTAINTY
Vladimir Ninković, Faculty of Security Studies, University of Belgrade, Serbia 36

PUBLIC-PRIVATE PARTNERSHIP IN CRITICAL INFRASTRUCTURE PROTECTION – STATUS AND DEVELOPMENT PERSPECTIVES IN THE REPUBLIC OF SERBIA
Nenad P. Radivojević, Advanced Cyber Security DOO, Serbia
Jana M. Marković, Faculty of Security Studies, University of Belgrade, Serbia...37

CRIMINAL LAW ASPECTS OF THE MISUSE OF AI AND TRANSFORMATIVE TECHNOLOGIES
Mile Šikman, Faculty of Law, University of Banja Luka, Bosnia and Herzegovina 38

CRITICAL INFRASTRUCTURE RISKS AND EARLY WARNING SYSTEMS: A COMPARATIVE REVIEW OF BALKANS PRACTICES
Marko Selaković, S P Jain London School of Management London, United Kingdom
Dimitrije Selaković, Universita Ca` Foscari Venice, Italy.....39

INTEGRATED CBRN RISK MANAGEMENT FOR CRITICAL INFRASTRUCTURE RESILIENCE
Marina Dabetić, "Vinča" Institute of Nuclear Sciences - National Institute of the Republic of Serbia, University of Belgrade, Serbia
Milica Ćurčić, "Vinča" Institute of Nuclear Sciences - National Institute of the Republic of Serbia, University of Belgrade, Serbia
Ivana Perović, "Vinča" Institute of Nuclear Sciences - National Institute of the Republic of Serbia, University of Belgrade, Serbia.....41

THE FUTURE OF CRITICAL INFRASTRUCTURE PROTECTION IN MONTENEGRO – THE NEW LAW ON THE RESILIENCE OF CRITICAL INFRASTRUCTURE AND ITS ALIGNMENT WITH THE EU LEGAL FRAMEWORK
Ivan Jeknić, Faculty of Political Science, University of Montenegro, Montenegro.....42

Preface

It is our honour to present the Book of Abstracts of the 4th International Conference on Critical Infrastructure (SKI 26), "Resilience of the Republic of Serbia's Critical Infrastructure at the Intersection of Geopolitics, Artificial Intelligence and Climate Change," taking place on November 5–6, 2026, at Zlatibor, Serbia.

This volume brings together contributions from researchers and practitioners concerned with the resilience of critical infrastructure and the continuity of essential services. Against a background of geopolitical uncertainty, rapid technological development, and climate-related pressures, the conference provides a platform for exchanging knowledge, discussing shared challenges, and connecting research with institutional and operational needs.

The abstracts collected in this volume cover a range of topics, including geopolitical and energy security, artificial intelligence and digital transformation, climate risks, and integrated approaches to infrastructure resilience. They address theoretical questions and practical challenges, including cybersecurity, adaptive crisis planning, early warning, crisis communication, public–private cooperation, and CBRN risk management. Regulatory and ethical considerations are addressed throughout these themes, highlighting the importance of human oversight, institutional responsibility, and coordination across sectors and borders.

The conference is organised by the Center for Risk Analysis and Crisis Management, with the support of the Ministry of Science, Technological Development and Innovation of the Republic of Serbia. Its co-organisers are the Faculty of Security Studies, University of Belgrade; the Institute for Standardization of Serbia; the Institute of International Politics and Economics; the Institute for Political Studies; the Atlantic Council of Montenegro; Singidunum University; HUB201; and the Jaroslav Černi Water Institute. We are grateful to the supporting institutions, partners, and organising and technical teams for their contributions to making this conference possible.

We extend our sincere thanks to all authors and participants for their contributions to the conference and this volume. We hope that this collection will serve as a useful reference for the discussions in Zlatibor and encourage continued collaboration, further research, and practical improvements in critical infrastructure resilience in Serbia and the wider region.

Editors

Zoran Keković, PhD,

University of Belgrade,

Faculty of Security Studies

Marina Dabetić, PhD, University of Belgrade, "Vinča" Institute of Nuclear Sciences - National Institute of the Republic of Serbia

Belgrade, November 2026

CHAPTER 1:
GEOPOLITICS AND CRITICAL INFRASTRUCTURE RESILIENCE

Şebnem Udum, Department of International Relations, Hacettepe University, Ankara, Türkiye[1)]

SECURITY OF NUCLEAR POWER PLANTS UNDER THE SHADOW OF GEOPOLITICAL SHIFTS

Nuclear power plants (NPPs) are critical energy infrastructure whose security depends not only on physical protection measures but also on the wider geopolitical environment. Intensifying interstate conflicts, changing regional power balances, and uncertainty surrounding security commitments challenge established assumptions about the protection of nuclear facilities. This paper examines how geopolitical shifts reshape the nuclear security threat assessment through two cases: Russia's war against Ukraine and the confrontation involving Iran, Israel, and the United States. The first case explores the implications of Russia's war against Ukraine for the security of nuclear power plants in an active conflict zone. The occupation of the Zaporizhzhia Nuclear Power Plant, military activities around nuclear facilities, and threats to supporting energy infrastructure demonstrate how interstate warfare can undermine established security arrangements and expose the limitations of conventional approaches to protecting nuclear installations. The Ukrainian experience raises broader questions about the vulnerability of nuclear infrastructure when a state's territorial integrity and sovereign control are challenged by military force. In this case, the country and the wider region face the risk of a nuclear safety failure, which could have consequences similar to those of the Chernobyl disaster. The second case considers the implications of escalating confrontation involving Iran, Israel, and the United States for nuclear power infrastructure in the Gulf region. Beyond immediate military threats, the analysis examines the potential consequences of shifting regional power balances and uncertainty about the durability of US security guarantees for regional states that operate or plan to develop nuclear power programs. These developments invite a reassessment of the strategic assumptions underlying the protection of nuclear infrastructure in a region exposed to interstate rivalry and regional escalation. By comparing these cases, the paper argues that geopolitical shifts are not merely an external context for nuclear security; they can transform threat perceptions, expose strategic dependencies, and create vulnerabilities that nuclear security measures alone cannot address. The paper concludes by considering the implications for national nuclear security strategies and the resilience of critical energy infrastructure.

Keywords: *nuclear security, critical infrastructure, geopolitics*

[1)] usebnem@hacettepe.edu.tr

Nenad Stekić, Faculty of Security Studies, University of Belgrade, Serbia[2)]

SECURING THE INFRASTRUCTURE OF OTHERS? CHINA'S APPROACH TO CRITICAL INFRASTRUCTURE SECURITY AND ITS IMPLICATIONS FOR PARTNER STATES

China is one of the largest builders and technology suppliers of infrastructure in Southeast Europe, including Serbia, increasingly in digitalised, data-intensive and AI-enabled forms such as smart city systems, cloud services and telecommunications networks. Yet debates on critical infrastructure resilience rarely ask how China itself conceptualises the security of such infrastructure, and they often treat Chinese suppliers either as an obvious threat or as a neutral commercial actor. This paper examines the question through qualitative content analysis of key Chinese policy and legal documents: the Cybersecurity Law (2017), the Data Security Law (2021), the Regulations on the Security Protection of Critical Information Infrastructure (2021) and the Global Security Initiative Concept Paper (2023), complemented by AI governance instruments. It asks how these documents define critical infrastructure, whom they treat as a threat, and what roles they assign to the state, companies and control over data. The paper argues that China treats critical infrastructure security primarily as a matter of state sovereignty and data control, with a broad and flexible definition of what counts as critical, while presenting its international role as that of a neutral development partner. This produces a double tension. First, the domestic regime (state-led classification, security reviews, data localisation, extraterritorial provisions) is not mirrored in the conditions under which Chinese-built infrastructure operates abroad, where it falls under host-state law. Second, it diverges from the expectations of the EU framework, notably NIS2 and the Critical Entities Resilience Directive, to which Serbia as a candidate country is expected to align. The paper also considers whether this critique applies symmetrically to other external suppliers, and where the evidence ends and speculation about intent begins. It concludes by outlining implications for Serbian institutions that manage infrastructure built or equipped by Chinese companies, and proposes questions for procurement and risk assessment.

Keywords: *critical infrastructure, China, Serbia, data security, Global Security Initiative, resilience, geopolitics*

[2)] nenad.stekic@fb.bg.ac.rs

Nataša Stanojević, Institute of International Politics and Economics, Belgrade, Serbia[3)]
Gordana Mišev, Institute of International Politics and Economics, Belgrade, Serbia

RESILIENCE OF THE REPUBLIC OF SERBIA'S TRANSPORT AND LOGISTICS INFRASTRUCTURE TO GEOPOLITICAL DISRUPTIONS

Transport and logistics infrastructure is essential to the functioning of the state and the continuity of critical flows during crises. This paper examines the resilience of Serbia's transport and logistics system to geopolitical disruptions, and assesses its capacity to maintain priority functions when transport routes, supply chains, or other external conditions are disrupted. Based on an analysis of the system's current state, the study identifies key vulnerabilities: high dependence on road transport, technical limitations of the railway network, dependence of river transport on hydrological conditions, and the spatial concentration of logistics hubs. The paper defines critical minimum operating levels for road, rail, air, and river transport, as well as for storage capacities and logistics hubs, and links them to readiness indicators and warning thresholds. On this basis, it develops a phased response model that enables appropriate measures to be activated gradually as the system approaches its critical minimum. The study's main scientific and practical contribution is to link critical minimum operating levels, readiness indicators, warning thresholds, and phased responses within a framework for assessing and managing the resilience of the transport and logistics system.

Keywords: *critical infrastructure, transport and logistics infrastructure, geopolitical risks, critical minimum, readiness indicators, phased response, Republic of Serbia*

[3)] natasa.stanojevic@diplomacy.bg.ac.rs

Jadranka Polović, Libertas International University, Zagreb, Croatia[4)]

STRATEGIC MARITIME CHOKEPOINTS AND ENERGY SECURITY: UPDATING MAHAN'S SEA POWER THEORY IN THE CONTEMPORARY GEOPOLITICAL CONTEXT

In the contemporary international system, energy is one of the key strategic resources, and its availability directly affects economic stability, national security, and social stability. Since at least the mid-2010s, energy systems have been increasingly exposed to a range of risks, including geopolitical tensions and conflicts, trade restrictions, and significant physical and cyber threats, resulting in significant disruptions to global supply chains. The reliable functioning of energy infrastructure is of critical importance to virtually all sectors of the modern economy and to public services, which depend heavily on the continuous availability of various forms of energy. Consequently, the governance and protection of critical energy infrastructure have become integral to broader political, economic, and societal resilience.

The geopolitical dimension of energy security became particularly pronounced in 2026, when the military escalation involving the United States, Israel, and Iran resulted in significant disruptions to maritime traffic through the Strait of Hormuz. Bab el-Mandeb, the maritime passage connecting the Red Sea with the Gulf of Aden, represents another strategically important route for international trade and energy transportation and has, in recent months, been exposed to serious disruptions in maritime traffic. Consequently, disruptions at strategic maritime chokepoints can generate cascading effects on transportation and insurance costs, energy and food prices, and the functioning of global supply chains. The concentration of critical infrastructure for energy production, processing, and transportation in geopolitically unstable regions has created what analysts describe as a "perfect storm" of systemic risk exposure. Indeed, the weaponisation of energy has emerged as one of the most significant transformations in international relations in the twenty-first century.

The central thesis of this paper is that contemporary energy security reaffirms the relevance of Mahan's Sea Power theory, as the control and protection of strategic maritime routes and chokepoints remain key components of geopolitical and economic power. At the same time, the concentration of energy infrastructure

[4)] jpolovic@libertas.hr

and transportation routes in geopolitically unstable regions, amid the turbulent transformation of the international order, significantly increases the systemic vulnerability of global supply chains.

Keywords: *energy security, critical infrastructure, Mahan's Sea Power Theory, Maritime Chokepoints, geopolitical risk, global supply chains*

Mitko Arnaudov, Institute of International Politics and Economics, Belgrade, Serbia[5)]

Sanja Jelisavac Trošić, Institute of International Politics and Economics, Belgrade, Serbia

THE CHALLENGES WITHIN CRITICAL INFRASTRUCTURE, AS A POTENTIAL FOR PRAGMATIC WESTERN BALKANS INTEGRATION ON THE EU PATH

Ongoing challenges facing critical infrastructure, both globally and locally, require synchronized and coordinated cross-border action to address and resolve them. Thus, such challenges cannot be perceived exclusively at national level. In this context, the aim of this paper is to research the scope of possibilities that such challenges provide for both regional cooperation and European integration. Bearing in mind the pivotal role that political elites in the Western Balkans region have in the decision-making process, neoclassical realism will be applied in the theoretical background of the paper. On the other hand, systematic theories will challenge the position of neoclassical realists regarding leadership behavior and perception in foreign policy positioning. The main hypothesis is that critical infrastructure challenges can serve as a driver for sustainable regional cooperation and accelerated European integration. Using the methodology of official documents and media content analysis, a leading research question is: do the Western Balkan states' institutional frameworks prevail in the decision-making process over leadership perceptions?

Keywords: *challenges, critical infrastructure, Western Balkans, cooperation, integration*

[5)] mitko@diplomacy.bg.ac.rs

Nenad Šijaković, JSC Elektromreža Srbije, School of electrical engineering University of Belgrade[6)]
Branko Djordjević, JSC Elektromreža Srbije, School of electrical engineering University of Belgrade

ENERGY SOVEREIGNISM AND NATIONAL SECURITY

This paper analyzes the concept of energy sovereignism as a fundamental pillar of the national security of the Republic of Serbia under the conditions of geopolitical shifts and the global energy transition. Starting from the premise that energy and national security are inextricably linked, the paper thoroughly deconstructs the three core postulates of a sovereign energy policy: availability, affordability, and sustainability. A pivotal focus is directed toward the conducted comparative geopolitical analysis of sovereignty models among key global powers, revealing stark conceptual contrasts: from the resource pragmatism of the US and the commodity-based sovereignty of Russia, to China's centralized technological dominance and France's defense of nuclear independence, contrasting with the structural collapse of Germany's ideologically driven energy transition (Energiewende). Within this global mapping, Serbia's position — with an import dependency of approximately 40% — is identified as significantly more resilient than both the European Union average (57%) and the rest of the Western Balkans, which is slipping into energy dependency. Furthermore, the techno-economic justification for integrating nuclear energy into the national energy mix is elaborated. Concurrently, the paper exposes sophisticated mechanisms of hybrid warfare and asymmetric access to information deployed to externally influence the strategic development vectors of the domestic power system. The study analyzes in detail the phenomenon of instrumentalizing ecological narratives, the creation of structural dependency, and the activities of so-called "synthetic experts" and purpose-funded, media-branded entities that generate an atmosphere of engineering nihilism and eco-anxiety in the public sphere, aiming to marginalize authentic institutional expertise. Through a comprehensive comparative analysis of the legislative and security frameworks of leading global powers and blocs (the US, the Russian Federation, the PR of China, and the EU), the paper proves that developed systems treat energy sovereignism as a vital security interest. Based on the derived

[6)] nenad.sijakovic@ems.rs

conclusions, a "Serbian Model of Energy Sovereignty" is proposed, which includes examining the establishment of a National Institute for Energy Security.

***Keywords**: energy sovereignism, national security, hybrid warfare, nuclear energy, asymmetric information, synthetic experts, electrical power system, energy transition, comparative legislation*

Zoran Milosavljević, Institute for Political Studies, Serbia[7)]
Mirjana Landika, Pan-European University "Apeiron", Bosnia and Herzegovina

DETERMINANTS OF THE PROFILES OF MIGRANTS IN TRANSIT THROUGH THE WESTERN BALKANS – CLUSTER ANALYSIS

This research focuses on the determinants of continued migration among migrants in transit through the Western Balkans. The study's analytical framework relies on empirical data from the report "Western Balkans Migration Routes & Dynamics – May–July 2025," prepared by the International Organization for Migration (IOM). During the observed period, 2,680 migrants were surveyed across Albania, Bosnia and Herzegovina, Montenegro, Serbia, Kosovo, and North Macedonia. The empirical data cover demographics, motives for movement, modes of travel, and migration plans. The study will conduct a descriptive analysis, an analysis of associations using the chi-square (χ^2) test, and, finally, a cluster analysis. The aim of the analysis is to examine and present the sample data empirically, and subsequently to use the chi-square (χ^2) test to investigate associations between variables (age and travel group, education and travel group, country of origin and intended destination, sleeping outdoors and reliance on intermediaries/facilitators, and bus travel versus taxi travel), and perform a cluster analysis. Cluster analysis will group respondents according to the characteristics examined and develop migrant profiles. The findings may support more effective management of migration processes, particularly in relation to their political and economic dimensions.

Keywords: *migration, Western Balkans, transit, migrant profile, statistical analysis*
JEL classification: F22, O15, J61, C38

[7)] bigz40@hotmail.com

CHAPTER 2:
ARTIFICIAL INTELLIGENCE AND DIGITAL TRANSFORMATION OF CRITICAL INFRASTRUCTURE

Zoran Keković, Faculty of Security Studies, University of Belgrade, Serbia[8)]

CRISIS DECISION-MAKING UNDER UNCERTAINTY: THE ROLE OF ARTIFICIAL INTELLIGENCE IN STRENGTHENING CRITICAL INFRASTRUCTURE RESILIENCE

Modern critical infrastructure systems face growing uncertainty driven by geopolitical disruptions, climate extremes, technological risks, and complex cross-sector interdependencies. Under these conditions, critical infrastructure resilience increasingly depends on the ability of institutions and operators to make timely and accountable decisions, often based on incomplete information and under significant time pressure.

This paper examines the opportunities and limitations of artificial intelligence in crisis decision-making, particularly in enhancing situational awareness, risk assessment, crisis forecasting, and the evaluation of alternative courses of action. Building on the concept of Dynamic Adaptive Crisis Planning, it proposes an integrated approach combining human judgment, expert knowledge, and AI-driven analytical capabilities within a continuous process of assessment, decision-making, and adaptive response. Particular emphasis is placed on maintaining human oversight, institutional accountability, and organizational learning from crises as essential prerequisites for strengthening long-term critical infrastructure resilience.

Keywords: *critical infrastructure, resilience, crisis decision-making, uncertainty, artificial intelligence, dynamic adaptive crisis planning*

[8)] zkekovic@fb.bg.ac.rs

Nebojša Bačanin Džakula, Singidunum University[9)]
Zoran Keković, Faculty of Security Studies, University of Belgrade, Serbia

METAHEURISTIC OPTIMIZATION OF ASYMMETRIC XGBOOST FOR INTERPRETABLE IOT AND INDUSTRIAL IOT INTRUSION DETECTION

As digital systems grow more complex, organizations face rising risks from cyberattacks and operational disruptions. This talk introduces how Generative Adversarial Networks (GANs) and metaheuristic optimization methods can provide fresh solutions for cybersecurity and risk management. GANs can simulate realistic attack scenarios, generate synthetic data to strengthen training datasets, and improve anomaly detection. Metaheuristic algorithms inspired by nature and collective intelligence help fine-tune cybersecurity models, select the most relevant features, and adapt defenses to rapidly changing environments. By combining these two approaches, we can build more resilient intrusion detection systems, more accurate phishing and malware detection tools, and smarter risk assessment frameworks. Practical examples will show both the potential and the limitations of these methods, with a focus on how academic research and industry applications can work together to create adaptive, trustworthy, and deployable AI-driven security solutions.

Keywords: *cybersecurity, generative adversarial networks, risk management, metaheuristics*

[9)] nbacanin@singidunum.ac.rs

Marina Dabetić, "Vinča" Institute of Nuclear Sciences - National Institute of the Republic of Serbia, University of Belgrade, Serbia[10)]
Ema Kraktus, Ministry of Education, Serbia
Jadranka Miletić Vukajlović, "Vinča" Institute of Nuclear Sciences - National Institute of the Republic of Serbia, University of Belgrade, Serbia

CRISIS COMMUNICATION DURING CBRN INCIDENTS: SOCIAL MEDIA AND AI-GENERATED CONTENT

During chemical, biological, radiological and nuclear (CBRN) incidents, people need timely, clear and credible information to understand the risks and decide how to protect themselves. Social media help authorities reach affected communities quickly, but they also allow misleading information to spread. AI-generated images, videos, audio and text can make it harder to distinguish reliable guidance from fabricated messages, particularly when information is incomplete and events are unfolding rapidly. This study will examine how social media and AI-generated content can influence crisis communication during CBRN incidents, with a focus on public trust, risk perception and adherence to protective instructions. A scoping review will follow JBI methodology and be reported in accordance with PRISMA-ScR guidelines. Research directly addressing CBRN incidents will be considered separately from studies of other emergencies whose findings may be relevant to this context. The thematic analysis will explore how information is communicated, how misleading content is identified and addressed, and what evidence exists about public responses. It will distinguish observed effects from anticipated risks, and research findings from regulatory requirements and institutional recommendations. The study aims to develop an evidence-informed conceptual framework to help institutions plan communication, verify AI-generated content, and identify questions that require further empirical research.

Keywords: *CBRN incidents; crisis communication; social media; AI-generated content; misinformation; public trust; risk perception*

[10)] fmarina@vin.bg.ac.rs

Dragana Dabić, Institute of International Politics and Economics, Belgrade, Serbia[11)]
Jelica Gordanić, Institute of International Politics and Economics, Belgrade, Serbia
Ivana Dunjić, Institute of International Politics and Economics, Belgrade, Serbia

FROM NORMS TO PRACTICE: PROTECTING CRITICAL INFRASTRUCTURE IN SERBIA IN THE AGE OF ARTIFICIAL INTELLIGENCE

Critical infrastructure protection is increasingly shaped by geopolitical fragmentation and the rapid spread of artificial intelligence (AI). These trends expose new vulnerabilities. AI deepens dependencies on external technology providers and widens the digital divide between states that develop these technologies and those that rely on them. Governance in this field does not rest on a single international regime, but on a regime complex – a set of overlapping institutions that differ in scope and legal force. Drawing on regime theory, and in particular on the analysis of authority relations and institutional differentiation within regime complexes, this paper examines how Serbia is positioned within this complex. On the one hand, Serbia has committed to the voluntary UN norms of responsible state behaviour in cyberspace, which call on states to refrain from intentionally damaging critical infrastructure, protect their own critical infrastructure and ensure supply-chain integrity. On the other hand, the EU accession process obliges Serbia to align with binding rules under the NIS2 and Critical Entities Resilience Directive and the AI Act. The paper assesses whether this architecture provides consistent rules or leaves room for overlap and ambiguity, and what this means for Serbia's behavioural adjustment, understood as the translation of international commitments into domestic practice. Based on qualitative analysis of UN, EU and national documents, it maps how responsibilities are distributed among the state, infrastructure operators, technology providers and incident response teams. It argues that the main challenge lies not in the absence of norms but in their implementation, and that Serbia's resilience depends on clarifying responsibilities across this regime complex.

Keywords: *Critical Infrastructure Protection, Regime Complex, Cyber Norms, Artificial Intelligence, Digital Divide, Serbia*

[11)] ddabic@diplomacy.bg.ac.rs

Gil Baram, University of South Florida, Bellini College of AI, Cybersecurity and Computing, USA[12)]

AI-ENABLED CYBERCRIME

Artificial intelligence (AI) is often treated as a force multiplier for cybercriminals, narrowing the debate to techniques like AI-generated phishing, malicious code, and deepfakes. This paper argues that AI-enabled cybercrime should be understood as an ecosystem-level transformation. It compresses decision timelines, amplifies ambiguity, and erodes the boundaries among criminal, state-linked, and hybrid actors. This breaks three assumptions that incident response, regulatory disclosure, and law enforcement depend on: that response can proceed sequentially, that evidence can be verified, and that perpetrators can be classified. Evidence comes from three tabletop exercises held between December 2024 and December 2025 in the United States, Singapore, and Israel, with more than 60 senior practitioners from government, law enforcement, industry, and academia. The three jurisdictions organize cybersecurity governance differently, yet reflexive thematic analysis identifies five failure patterns that recurred at every site. These aggregate into three structural deficits: accountability gaps, coordination deficits, and ambiguity over decision rights. Recurrence across such different systems locates the problem beyond any organization's preparedness and calls for an ecosystem shift.

Key words: *AI; AI-enabled cybercrime; cybersecurity governance; incident response; regulatory disclosure; law enforcement; tabletop exercises; ecosystem resilience*

[12)] glbaram@gmail.com

Nikola Milivojević, Jaroslav Černi Water Institute, Belgrade, Serbia
Vladimir Milivojević, Jaroslav Černi Water Institute, Belgrade, Serbia[13)]
Ivana Krtolica, The Institute for Artificial Intelligence Research and Development of Serbia, Novi Sad, Serbia

AI ASSISTANTS IN WATER INFRASTRUCTURE MANAGEMENT: BOUNDARIES OF TRUST AND RESPONSIBILITY

AI assistants increasingly connect natural-language requests with information retrieval, engineering models and recommendations for critical water infrastructure. Their ability to produce coherent answers does not establish when those answers can justifiably influence an operational decision. This paper develops a conceptual framework linking trust boundaries, acceptance criteria and responsibility. A focused synthesis of water-sector applications, research on language-model reliability and human reliance, and cybersecurity and AI governance guidance identifies eight boundaries spanning source selection, instruction authority, model configuration, temporal applicability, interpretation, oversight, authorisation and implementation. The framework distinguishes acceptance for analytical use from approval for implementation and assigns verification duties to identifiable roles. Criteria are non-compensatory: a confirmed failure prevents the recommendation from being accepted for its intended use, while unresolved findings require further verification or escalation. Constructed operational scenarios illustrate how similar unsuitable recommendations can originate at different boundaries, how an altered instruction can fall outside an existing approval, and how ineffective oversight can permit erroneous approval. Accidental defects and deliberate manipulation are examined together at the level of decision integrity while their causes remain distinct. The framework relates justified reliance to the preservation of operating constraints and decision authority under disruption. Its contribution to infrastructure resilience remains to be tested through empirical evaluation of defect detection, finding resolution and prevention of unsupported implementation under representative working conditions.

Keywords: *large language models, critical infrastructure resilience, water infrastructure, trust boundaries, human oversight, digital twins*

[13)] vladimir.milivojevic@jcerni.rs

Inda Kreso, GEOPOL – Center for Geopolitical Research, Sarajevo, Bosnia and Herzegovina[14)]
Irma Sokolović, Woman4Cyber Bosnia and Herzegovina, Sarajevo, Bosnia and Herzegovina

RADIO FREQUENCY MONITORING FOR UAV DETECTION: A COMPARATIVE ANALYSIS OF TECHNOLOGIES AND CHALLENGES IN CRITICAL INFRASTRUCTURE PROTECTION

The increasing availability and use of unmanned aerial vehicles (UAVs) present new security challenges for critical infrastructure, including energy facilities, airports, telecommunications networks, and other strategically important installations. Detecting unauthorised drone activity has therefore become an important aspect of infrastructure protection and security risk management. Radio frequency (RF) monitoring is one of the approaches used to detect drones by identifying and analysing the communication signals associated with their operation.

This research examines the role, capabilities, and limitations of RF monitoring technologies in detecting UAVs and supporting critical infrastructure protection. Using a structured literature review and comparative analysis, the study explores existing detection approaches, including radio spectrum monitoring, signal identification, and automated detection methods. The analysis focuses on how these technologies contribute to detecting and identifying drones, their effectiveness in different operational environments, and the challenges that may affect their reliability.

The study aims to identify the main advantages and limitations of RF-based UAV detection, particularly in relation to signal interference, autonomous drone operations, and the difficulty of distinguishing potential threats from legitimate activities. By comparing existing approaches and examining their practical application, the research seeks to provide a clearer understanding of how RF monitoring can support early threat detection, security risk assessment, and the protection and resilience of critical infrastructure.

Keywords: *UAV, detection, radio frequency, critical infrastructure, monitoring*

[14)] indakreso@fkn.unsa.ba

Jelena Marković, Mozzart Foundation, Belgrade, Serbia[15)]

READINESS OF PRIMARY SCHOOLS IN SERBIA TO RESPOND TO CRITICAL INFRASTRUCTURE BREAKDOWN AND EMERGENCY SITUATIONS: AN EMPIRICAL ANALYSIS OF OCCUPATIONAL SAFETY AND HUMAN CAPITAL PROTECTION SYSTEMS

Primary schools are a key component of social infrastructure whose operational continuity relies on the stability of critical infrastructure. Disruptions to these systems caused by natural disasters or technical and technological accidents directly threaten the safety of children and staff as primary carriers of human capital. This study evaluates the readiness of primary schools in the Republic of Serbia to respond to disruptions and critical infrastructure breakdowns. It uses a mixed-methods triangulation approach, comprising secondary analysis (N=20 primary schools), semi-structured interviews (N=24), and a survey (N=525). Empirical findings reveal high formal compliance with statutory requirements alongside serious functional and operational shortcomings. Although 95% of schools have basic internal regulations, 85% have neither an internal occupational health and safety strategy nor a first-aid rulebook. Approximately 70% of schools allocate no funds to preventive risk management, while 12% have not provided employees with basic emergency-response training. Training continuity is also a major concern: 85% of schools lack both a dedicated budget and up-to-date educational materials. Coordination with local emergency-management headquarters and state authorities remains predominantly reactive. Although primary schools in Serbia meet baseline legal requirements, they remain vulnerable to critical infrastructure breakdowns because of missing emergency protocols, insufficient investment, and limited practical preparedness among staff. Revising risk-assessment documents, introducing mandatory practical training, and integrating school systems more fully into critical infrastructure protection plans are essential next steps.

Keywords: *critical infrastructure, primary schools, occupational health and safety, human capital, emergency situations*

[15)] jelena.markovic@mozzartbet.com

Lepa Babić, Singidunum University[16)]

ARTIFICIAL INTELLIGENCE GOVERNANCE AND ALIGNMENT WITH ETHICAL PRINCIPLES IN HEALTHCARE

The accelerating digitalisation of healthcare systems and the expanding use of artificial intelligence (AI) in clinical practice raise critical questions about governance and ethical frameworks. In 2021, the World Health Organization identified six core principles for AI in health: protecting human autonomy, promoting well-being and safety, ensuring transparency and explainability, fostering accountability, ensuring inclusiveness and equity, and promoting responsive and sustainable AI. At the European Union level, the AI Act (Regulation 2024/1689) introduces a binding risk-based framework. Diagnostic tools, clinical decision-support systems, and patient-monitoring applications are classified as high-risk AI, triggering obligations for data governance, technical documentation, human oversight, and post-market performance monitoring. The Medical Device Regulation (MDR 2017/745) and standards ISO 13485 and ISO 14971 complement this framework. Significant practical challenges persist: insufficiently defined transparency standards for black-box models; inconsistent conformity assessment procedures across EU member states; unclear allocation of liability among developers, hospitals, and clinicians; and automation bias — the tendency of clinicians to place excessive trust in AI recommendations at the expense of their own clinical judgement. This paper proposes an integrated governance model encompassing regulatory compliance with the EU AI Act and WHO ethical guidelines, technical measures such as audit trails, model cards, and real-time performance dashboards, and multidisciplinary ethics committees as an institutional mechanism. The framework's applicability is considered in the context of Serbia's healthcare system and the national AI Development Strategy for 2024-2030, accounting for the obligation to align domestic legislation with EU regulation.

Keywords: *AI governance, healthcare ethics, EU AI Act, WHO guidelines, transparency, accountability, high-risk AI systems, medical devices*

[16)] lbabic@singidunum.ac.rs

Bogdan Filipović, "Živko Ljujić" Primary School, Serbia[17)]

CASE STUDY: AI, HUMAN DIGNITY AND GLOBAL RISKS

A student wrote her Serbian language essay using AI. The teacher believed that the student had used AI and refused to grade the assignment. If the student had used AI, she would have been held accountable for a school rule violation: misusing AI for fraud. If she had written the essay independently, without AI, the teacher would face accusations of violating the student's dignity.

How great is the leap from potential cheating on a high school essay to using AI for much larger-scale fraud with unimaginable consequences?

Keywords: *artificial intelligence, human dignity, global risks*

[17)] bogdan.filipovic@gmail.com

Ivana Vlašković, Institute for Political Studies, Belgrade, Serbia[18)]

REGULATORY TRANSFORMATION OF CRITICAL INFRASTRUCTURE IN THE ERA OF ARTIFICIAL INTELLIGENCE: THE EUROPEAN FRAMEWORK AND THE PERSPECTIVE OF SERBIA

Artificial intelligence is reshaping how critical infrastructure is operated, monitored, and protected. It opens new capabilities for automated risk assessment, early warning, real-time monitoring, and incident prediction, while introducing new security exposures, risks of misuse, and unresolved regulatory and ethical questions. As critical infrastructure becomes increasingly digitalized and dependent on autonomous and semi-autonomous systems, the governance of AI shifts from a technical concern to a core dimension of infrastructure resilience. Against this backdrop, the European Union regulates AI through a risk-based approach, imposing specific obligations on high-risk systems, a category that directly encompasses many critical-infrastructure applications. The AI Act, together with the NIS2 and Critical Entities Resilience (CER) Directives, forms part of a broader regulatory transformation aimed at securing infrastructure that increasingly relies on intelligent and automated systems. Theoretically, the paper draws on the concept of Normative Power Europe (Manners), which frames the EU as an actor that shapes international standards through the diffusion of its norms, and applies a normative-legal method to analyze how these norms reshape domestic regulatory obligations in Serbia within the European integration process. The central research question is: how does the EU regulatory framework for artificial intelligence change the requirements for the protection and management of critical infrastructure, and what challenges does alignment pose for Serbia? Methodologically, the research combines qualitative content analysis of key documents, including the AI Act, the NIS2 and CER Directives, the Artificial Intelligence Development Strategy of the Republic of Serbia 2025–2030, and the Law on Critical Infrastructure, with comparative analysis of regulatory solutions and standards. The paper argues that, as a normative power, the EU reframes critical infrastructure protection around the trustworthiness and controllability of AI systems, and that Serbia's alignment poses challenges of institutional capacity, technical standardization, and regulatory sequencing, while identifying key directions and opportunities for their transposition.

Keywords: *artificial intelligence, critical infrastructure protection, EU AI act, normative power Europe, regulatory alignment, Serbia*

[18)] ivana.vlaskovic@ips.ac.rs

CHAPTER 3:
CLIMATE CHANGE, EXTREME EVENTS AND CRITICAL INFRASTRUCTURE RESILIENCE

Velimir Strugar, Directorate for IMS and General Affairs, Nikšić, Montenegro[19)]

ARTIFICIAL INTELLIGENCE, CLIMATE RISK AND CRITICAL INFRASTRUCTURE: ETHICAL ASPECTS OF RESPONSIBILITY AND HUMAN OVERSIGHT IN AUTOMATED DECISION-MAKING

Heatwaves, droughts, floods and wildfires are becoming more frequent and more severe, and they place growing stress on critical infrastructure. Operators respond in part by introducing artificial intelligence (AI) for forecasting, early warning, anomaly detection and automated control. AI is thus deployed in situations where extreme events leave operators little time to deliberate, and the ethical questions it raises cannot be separated from climate risk. Taking the consequentialist, deontological and virtue ethics traditions as a starting point, the paper discusses four problems of AI-supported resilience, with examples from energy systems. Automated load shedding and restoration priorities distribute harm among users, which raises the question of whether operators, technology vendors or public authorities should set the rules such systems follow. When a failure results from the interaction of autonomous functions, operators and suppliers, it may be unclear who is responsible. Models trained on historical data lose reliability as the climate changes, since past observations say less about future extremes, and an error in a widely used model can affect the whole system. Finally, routine automation erodes the practical skills operators need when automated systems fail. The paper argues that ethical assessment of AI in critical infrastructure should be specific to the domain and part of resilience planning. It proposes principles of human oversight, transparency and accountability and examines them against the EU AI Act, the CER and NIS2 Directives, relevant ISO/IEC standards, and the national legislation of Serbia and Montenegro on critical infrastructure and information security.

Keywords: *critical infrastructure resilience, artificial intelligence, ethics, climate change, human oversight, energy systems*

[19)] velimir.strugar@epcg.com

Nenad Šijaković, JSC Elektromreža Srbije, School of electrical engineering University of Belgrade, Serbia[20)]
Branko Djordjević, JSC Elektromreža Srbije, School of electrical engineering University of Belgrade, Serbia
Branislav Djukić, Electricity Coordinating Center - EKC, Belgrade, Serbia

THE PARADIGM OF RESILIENCE AND CONTROLLED DEVELOPMENT OF THE ELECTRICAL POWER SYSTEM IN THE ERA OF CLIMATE EXTREMES AND HYBRID GEOPOLITICAL PRESSURES

Modern electrical power systems (EPS) face synergistic pressures from climate extremes and hybrid geopolitical actions. This paper deconstructs the traditional, conventional "4A" model of energy security and demonstrates its static insufficiency within the modern security context. In response, the authors introduce a critical fifth dimension—Resilience (Systemic Resilience)—defined as the engineering and technological capacity of the grid and generation mix to absorb external shocks without disrupting the core operational parameters of the EPS. In light of the amendments to the Energy Act (2024), this study analyzes three tiers of measures designed to safeguard the security of supply in the Republic of Serbia. Particular emphasis is placed on the necessity of drafting and updating the Risk-Preparedness Plan, properly assessing regional and national crisis scenarios for effective real-time crisis management, and the strategic long-term planning of a national generation mix tailored to the specific characteristics, economic architecture, and geopolitical reality of the Republic of Serbia. Particular attention is given to the strategic justification for lifting the moratorium on nuclear energy for peaceful purposes, alongside the introduction of the "Iron Reserve" concept for lignite as a final line of defense for national sovereignty, envisioned within future overarching national strategic documents. The paper concludes that rigid, long-term strategic centralized planning of the national generation mix—enforced through strictly regulated state quotas, a clear institutional chain of accountability, and rigorous oversight regarding the realization of strategic national generation assets—constitutes a fundamental prerequisite for preserving the national economy and overall national security.

Keywords: *security of supply, national security, risk-preparedness plan, crisis scenarios, iron reserve, strategic planning, state realization control*

[20)] nenad.sijakovic@ems.rs

Gjorgji Alceski, TAV Macedonia, Ohrid St. Paul the Apostle Airport, Ohrid, North Macedonia[21)]

APPLICATION AND LIMITATIONS OF ARTIFICIAL INTELLIGENCE (AI) IN AVIATION SECURITY (AvSec)

The use of artificial intelligence (AI) is increasing across the aviation sector. Airport operators, airlines, aviation service providers, manufacturers, aviation authorities, and training organisations are increasingly relying on AI tools. By adopting these technologies while addressing the associated risks, airports can better respond to growing passenger volumes and improve the travel experience for all.

Artificial intelligence is emerging not only as an analytical tool but also as a predictive tool in management systems. AI and data are no longer "future topics" in aviation; integrating AI tools with operational and security data offers significant potential from operational, technological, control, and security perspectives.

AI technology can help airports improve operations and safety, including aviation security (AvSec). AI analytics systems are becoming proactive security systems for real-time security threat recognition and decision-making. These systems can significantly improve airport management, improve operational efficiency, enhance passenger experience and strengthen airport safety and security.

The increasing application of AI also requires responsibilities, including regulation, control, oversight, application models, restrictions, etc. as well as strict compliance with regulatory frameworks from international institutions such as EASA, FAA, ICAO and be independently validated and certified before being implemented in safety-critical aviation environments.

Regarding the fact that artificial intelligence has a potential to revolutionize airport operations, improve safety and security, increase passenger satisfaction and increase overall efficiency, this paper will attempt to answer the question how and to what extent can we use artificial intelligence in the area of Aviation security (AvSec) and what are the limitations related to the reliability of decision-making, the degree of independence of the systems as well as the protection of privacy and personal data?

Keywords: *aviation security, safety, artificial intelligence, limitations and applicability*

[21)] gjorgji.alcheski@tav.aero

Sanja Grbović, Faculty of Law, University of Montenegro, Podgorica, Montenegro[22)]

BEYOND PROTECTION: THE EU'S 2026 GUIDELINES ON CRITICAL ENTITIES RESILIENCE

The protection of critical infrastructure has increasingly evolved beyond traditional security-oriented approaches towards a broader understanding of resilience, encompassing prevention, preparedness, continuity of essential services, and recovery from disruptive incidents. Against this background, the European Commission's Guidelines of July 2026 on the application of Article 13(5) of Directive (EU) 2022/2557 represent an important development in the operationalisation of the EU's regulatory framework for critical entities.

This paper examines whether, and to what extent, these non-binding Guidelines contribute to redefining critical infrastructure resilience within EU law. Through doctrinal and critical legal analysis, it explores the relationship between the legally binding obligations established by the Critical Entities Resilience Directive and the interpretative and operational guidance subsequently provided by the Commission. The analysis argues that, although the Guidelines do not formally alter the existing legal framework, their significance extends beyond technical clarification. By translating broadly formulated obligations into more concrete preventive, organisational, and recovery measures, they may influence how resilience is understood and implemented across Member States. At the same time, their non-binding character raises questions concerning legal certainty, regulatory consistency, and the limits of soft law in achieving a harmonised approach to critical infrastructure resilience.

The paper contributes to the broader debate on EU regulatory governance by examining whether the effectiveness of resilience regulation depends not only on the adoption of binding legal standards, but also on their progressive operationalisation through complementary instruments.

Keywords: *critical infrastructure, critical entities resilience, European Union law, 2026 Commission guidelines, soft law, regulatory governance*

[22)] sanjag@ucg.ac.me

CHAPTER 4:
AN INTEGRATED APPROACH TO CRITICAL INFRASTRUCTURE RESILIENCE IN THE REPUBLIC OF SERBIA

Vladimir Ninković, Faculty of Security Studies, University of Belgrade, Serbia[23)]

DYNAMIC ADAPTIVE CRISIS PLANNING: A CONCEPTUAL FRAMEWORK FOR CRISIS RESPONSE UNDER DEEP UNCERTAINTY

Crisis plans are developed before the conditions of an actual disruption are known and may become inadequate as a crisis evolves. This conceptual article proposes a framework for dynamic adaptive crisis planning (DACP) by selectively translating principles from Dynamic Adaptive Planning, Dynamic Adaptive Policy Pathways, and their multi-risk and multidimensional extensions into organizational crisis response. The framework links an initial response to critical assumptions, signposts, triggers, contingent actions, response pathways, decision authority, and fundamental reassessment. It is designed to help organizations recognize when a response is becoming inadequate and adapt it under deep uncertainty without displacing professional judgment or bounded improvisation. DACP may thereby contribute to second-order resilience. As the framework remains conceptual, its feasibility, usability, and organizational effects require examination through exercises and a subsequent empirical pilot study.

Keywords: *dynamic adaptive planning, crisis plans, organizational resilience, decision-making, deep uncertainty*

[23)] vladimir.ninkovic@fb.bg.ac.rs

Nenad P. Radivojević, Advanced Cyber Security DOO, Serbia[24)]

Jana M. Marković, Faculty of Security Studies, University of Belgrade, Serbia

PUBLIC-PRIVATE PARTNERSHIP IN CRITICAL INFRASTRUCTURE PROTECTION – STATUS AND DEVELOPMENT PERSPECTIVES IN THE REPUBLIC OF SERBIA

Public-Private Partnership (PPP) is increasingly becoming a paradigm of development in modern countries. Although fundamentally an economic concept, PPP is becoming a model that finds its application in the field of critical infrastructure protection (CIP). As a country aspiring to membership in the European Union, the Republic of Serbia is required to harmonize its regulations with the EU acquis on CIP. One of the basic mechanisms in this field is PPP, which implies cooperation between private and public actors. In addition to the dominant economic aspect, PPP can also be viewed from the security aspect, integrating the forces and means of the private and public sectors through exchange of information, joint training, joint and coordinated action in regular and crisis situations, development of risk assessments and security plans, etc. The starting assumption is that this issue is in the Republic of Serbia regulated in principle by the Law on Critical Infrastructure, the Law on Private Security, as well as other relevant regulations. Accordingly, this paper analyzes the relevant positive legal framework, to determine whether the security aspect of PPP is regulated and implemented in security practice. The initial analysis indicates that PPP in the Republic of Serbia is recognized as a model for the development and construction of the infrastructure itself, while the security aspect of this partnership is fragmented and insufficiently normatively regulated. The strictly economic aspect of PPP can significantly contribute to the financing and construction of critical infrastructure (CI), technological modernization of society, which is certainly important for the overall increase in the resilience of the CI. At the same time, further development and normative conceptualization of PPP in the field of security protection are necessary. Accordingly, based on an analysis of the existing legal framework, the paper puts forward certain de lege ferenda proposals.

Keywords: *critical infrastructure, protection of critical infrastructure, public-private partnership, police, private security*

[24)] n.radivojevic@pf.uns.ac.rs

Mile Šikman, Faculty of Law, University of Banja Luka, Bosnia and Herzegovina[25)]

CRIMINAL LAW ASPECTS OF THE MISUSE OF AI AND TRANSFORMATIVE TECHNOLOGIES

The emergence of generative and transformative Artificial Intelligence (AI) radically alters the nature of committing criminal offenses, creating a legal vacuum between the incrimination of new forms of delicts and the allocation of criminal liability itself. This phenomenon cannot be viewed merely as a quantitative increase in the volume of offenses, but rather as a qualitative mutation of the very substratum of criminal behavior, posing unprecedented challenges to criminal law theory and legislation. Data has become both the primary legal object of protection and the fundamental tool of execution. AI systems are currently utilized for intelligent mapping and automated extraction of structured personal, financial, or state databases. Beyond unauthorized access, new delicts are emerging, such as data poisoning, the deliberate injection of malicious information into AI training datasets to induce systemic collapse or biased decision-making. Furthermore, the introduction of new technologies has not eliminated classical delicts but has digitally transformed them through AI-generated attacks that target victims with incredible precision. Within the economic sphere, the misuse of blockchain technologies has led to specific forms of financial crime (primarily money laundering), along with new execution methods involving the abuse of Smart Contracts and manipulation within decentralized financial markets (DeFi scams), which conventional corporate crime doctrines fail to encompass. Operating as a criminogenic ecosystem, the Darknet provides a parallel digital economy protected by advanced anonymity and encryption protocols. Meanwhile, the criminal and civil liability of chat bots and advanced AI systems, amidst the disruption of traditional causal links, remains one of the most complex and pressing issues in contemporary legal science.

Keywords: *artificial intelligence, transformative technologies, data poisoning, smart contracts, darknet, criminal liability*

[25)] mile.sikman@pf.unibl.org

Marko Selaković, S P Jain London School of Management London, United Kingdom[26)]
Dimitrije Selaković, Universita Ca` Foscari Venice, Italy

CRITICAL INFRASTRUCTURE RISKS AND EARLY WARNING SYSTEMS: A COMPARATIVE REVIEW OF BALKANS PRACTICES

This study compares early warning system (EWS) practices for critical infrastructure risks across the Balkans, with a focus on Serbia and neighbouring countries. It examines how pre-crisis warnings, acute crisis response, and post-crisis recovery are designed, communicated, and coordinated institutionally in the context of current BANI-world challenges. The central research question is: Which EWS and risk-communication approaches demonstrate resilience, and what can Serbia adopt for a national critical infrastructure resilience model? Drawing on international best practices and examples from Balkan countries, the paper argues that proactive and transparent pre-crisis communication reduces physical and reputational losses, while ambiguous messages during and after a crisis can cause further confusion and increase risks to critical infrastructure.

The study uses a comparative document and policy analysis of national risk assessments, civil protection and critical infrastructure laws, EWS strategies, progress reports, regional cooperation mechanisms, and publicly available crisis communication examples from major floods, earthquakes, and wildfires that happened in the Balkan countries between 2014 and 2026. It applies a three-phase analytical framework derived from Situational Crisis Communication Theory and risk communication research, distinguishing pre-crisis warning and preparedness, crisis response coordination, and post-crisis rebuilding and learning. Sources include governmental, intergovernmental, operator, and media communications from Serbia, Croatia, Romania, Bulgaria, Montenegro, Bosnia and Herzegovina, and North Macedonia. The analysis focuses on five dimensions: risk detection and warning dissemination, message clarity and public comprehension, information exchange, cross-border interoperability, and post-crisis feedback loops.

The review finds fragmented and uneven EWS practices across the Balkans. While some aspects of show progress, especially where EU accession and civil protection funding support modernization, real-time cross-border data exchange and

[26)] marko.selakovic@spjain.ac.uk

standardized protocols are still underdeveloped. Warning dissemination is frequently multimodal, but inconsistent: certain jurisdictions operate modern cell-broadcast or app-based alerts, while others still rely heavily on traditional mass warning systems, television, and social media. Thus, unequal message reach to various groups is noticeable. Critical infrastructure operators and systems are frequently outside unified public alert loops. Pre-crisis communication is generally less systematic than in-crisis and post-crisis messaging, resulting in reactive rather than anticipatory action. AI-supported multi-hazard platforms are piloted in some countries but are not systematically embedded in critical infrastructure risk management. Countering disinformation and low public trust remain significant challenges, especially where governments fail to provide timely and actionable instructions.

The results suggest that Serbia's emerging national model should treat early warning as a comprehensive crisis communication system with clear roles, standardized messages, and mandatory operator integration. Pre-crisis investments in interoperable regional EWS, multilingual and accessible alerts, AI-enabled predictive analytics, and public education must be viewed as a point of emphasis for the improvement of the Serbian national model. During crises, government-to-operator and government-to-public messaging must be unified and unambiguous, and recovery framing must not be issued before critical services are genuinely restored. Post-crisis actions should institutionalize after-action reviews, transparent communication, and clearly defined learning loops. Observing from the Balkans perspective, enhanced regional cooperation can help overcoming technical limitations, geopolitical asymmetries (EU vs. Non-EU), and build common situational awareness.

Keywords: *critical infrastructure, crisis communication, crisis risks, early warning systems, natural disasters*

Marina Dabetić, "Vinča" Institute of Nuclear Sciences - National Institute of the Republic of Serbia, University of Belgrade, Serbia[27)]
Milica Ćurčić, "Vinča" Institute of Nuclear Sciences - National Institute of the Republic of Serbia, University of Belgrade, Serbia
Ivana Perović, "Vinča" Institute of Nuclear Sciences - National Institute of the Republic of Serbia, University of Belgrade, Serbia

INTEGRATED CBRN RISK MANAGEMENT FOR CRITICAL INFRASTRUCTURE RESILIENCE

Chemical, biological, radiological and nuclear (CBRN) incidents can threaten human health and the environment while disrupting essential services. Managing these risks requires coordination between emergency services, public authorities, critical infrastructure operators and affected communities across prevention, preparedness, response and recovery. This paper aims to examine how an integrated approach to CBRN risk management can support critical infrastructure resilience, with particular attention to interinstitutional coordination, preparedness and continuity of essential services.

The study will combine a narrative review of scientific literature with a qualitative analysis of selected institutional guidance documents. The analysis will consider the integration of proactive and reactive approaches across risk assessment, prevention, mitigation, preparedness, response and recovery. Particular attention will be paid to cooperation among public authorities, emergency services, infrastructure operators and local communities, including information sharing, joint planning and the clarification of operational responsibilities. Drawing on the reviewed approaches, the paper will explore the role of modelling and scenario-based simulation exercises in identifying vulnerabilities, assessing resource needs and testing emergency plans and procedures. These tools will be considered in relation to both the immediate management of CBRN incidents and the maintenance and restoration of essential services. Public communication, community participation and the incorporation of lessons learned will also be examined as components of an adaptive management process. The intended contribution is a conceptual framework linking the phases of CBRN risk management with institutional responsibilities, operational capabilities and critical infrastructure resilience objectives. The framework will provide a basis for identifying priorities for coordination, training and further empirical evaluation.

Keywords: *CBRN risk management, disaster risk reduction, critical infrastructure, resilience, interinstitutional coordination, simulation exercises*

[27)] fmarina@vin.bg.ac.rs

Ivan Jeknić, Faculty of Political Science, University of Montenegro, Montenegro[28)]

THE FUTURE OF CRITICAL INFRASTRUCTURE PROTECTION IN MONTENEGRO – THE NEW LAW ON THE RESILIENCE OF CRITICAL INFRASTRUCTURE AND ITS ALIGNMENT WITH THE EU LEGAL FRAMEWORK

The paper examines the recently adopted Law on the Resilience of Critical Infrastructure in Montenegro, focusing on the quality and applicability of its provisions and their alignment with EU rules and standards. The author analyzes this new legislation in terms of good regulatory practice, delving into the reasons and explanations for certain regulatory solutions found in its provisions. The paper then explores how the new Law aligns with the current EU framework, primarily with the Critical Entities Resilience Directive, as this new legal act has been adopted explicitly to implement this Directive, but also with other Montenegrin and EU legislation concerning critical infrastructure protection. Specifically, the author examines whether the Law takes into account the aims and requirements of the CER Directive, instead of simply copying the provisions of the Directive without regard to the national context - the characteristics and needs of CI protection in Montenegro, the public administration and other relevant institutions. The author concludes with recommendations for improving the new legislation and supporting effective implementation of both the Law and the Directive.

Keywords: *law on the resilience of critical infrastructure*, *Montenegro*, *CER Directive*, *critical infrastructure protection*, *resilience*

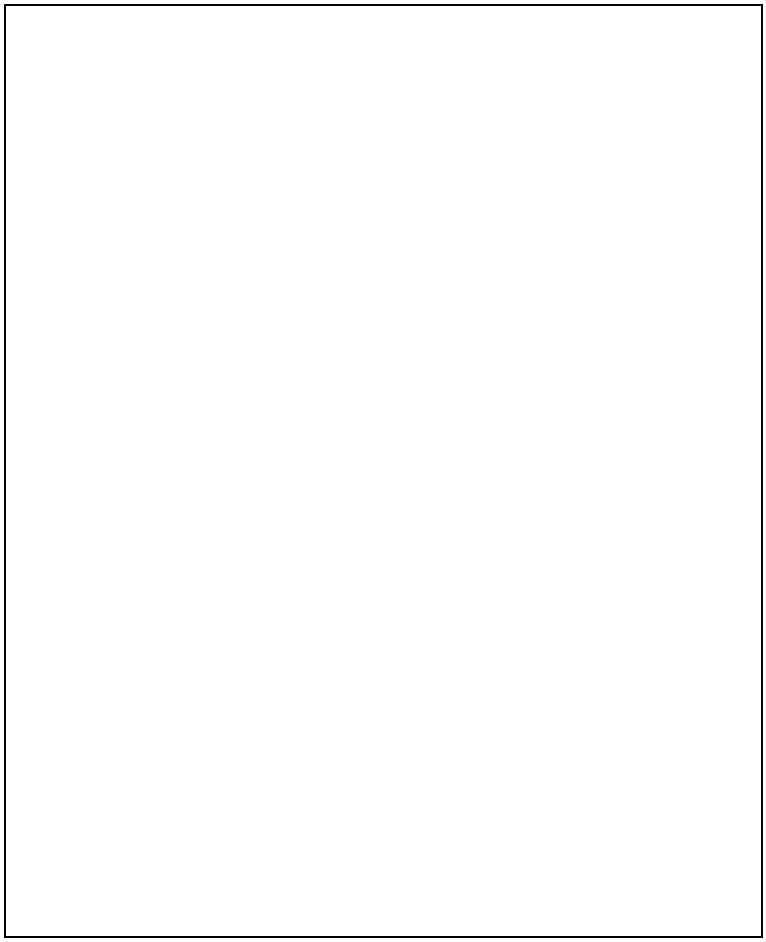
[28)] ivan.jeknic@gmail.com



center

for risk analysis and
crisis management

CIP - Каталогизација у публикацији
Народна библиотека Србије, Београд



Publisher:
Center for Risk Analysis and Crisis Management with the support of
Ministry of the Science, Technological Development and Innovation
of the Republic of Serbia

ISBN 978-86-909840-0-8