Conference Book Of Abstracts

INTERNATIONAL SCIENTIFIC AND PROFESSIONAL CONFERENCE:

CRITICAL INFRASTRUCTURE SYSTEMS IN THE ERA OF ARTIFICIAL INTELLIGENCE

CIS-AI NEXUS - CONVERGENCE OF CRITICAL INFRASTRUCTURE AND ARTIFICIAL INTELLIGENCE

17-18 October 2024, Belgrade, Serbia

The Center for Risk Analysis and
Crisis Managmenet - Belgrade
www.caruk.rs

INTERNATIONAL SCIENTIFIC AND EXPERT CONFERENCE:

CRITICAL INFRASTRUCTURE SYSTEMS IN THE ERA OF ARTIFICIAL INTELLIGENCE

CIS-AI NEXUS – CONVERGENCE OF CRITICAL INFRASTRUCTURE AND ARTIFICIAL INTELLIGENCE

Conference Book of Abstracts

Conference is supported by the Ministry of Education, Science and Technological Development of the Republic of Serbia

Republic of Serbia
MINISTRY OF SCIENCE,
TECHNOLOGICAL DEVELOPMENT AND INNOVATION

ISBN 978-86-902810-7-7

Serbia, 2024

Conference Book of Abstracts

INTERNATIONAL SCIENTIFIC AND EXPERT CONFERENCE:

CRITICAL INFRASTRUCTURE SYSTEMS IN THE ERA OF ARTIFICIAL INTELLIGENCE

CIS-AI Nexus – CONVERGENCE IN CRITICAL INFRASTRUCTURE AND ARTIFICIAL INTELLIGENCE
October 17-18 October, 2024

Published by:
Center for Risk Analysis and Crisis Management

Editor:
Prof. dr Zoran Keković, PhD, University of Belgrade, Faculty of Security Studies

Proofreading:
Ljubica Petrović

Text wrapping:
Snežana Trajković

Printed by:
Data Copy, Novi Beograd

Copies: 100

Belgrade, October 2024

ORGANIZATIONAL COMMITTEE:

Zoran Keković, PhD, University of Belgrade, Faculty of Security Studies

Tatjana Bojanić, Institute for Standardization of Serbia, Director

Biljana Abolmasov, PhD, University of Belgrade, Faculty of Mining and Geology

Aneta Spaić, PhD, University of Montenegro, Faculty of Law

Nikola Milivojević, PhD, Jaroslav Černi Water Institute, Belgrade, Serbia

Milan Stojković, PhD, Institute for Artificial Intelligence Research and Development of Serbia, Novi Sad, Serbia

Dragan Radulović, The Association of Security Managers of Montenegro, President

REVIEWERS:

Aleksandar Jovanović, CEO Steinbeis EU-VRi (Steinbeis European Risk & Resilience Institute), Stuttgart, Germany, Associate Member ETH Risk Center, ETH Zürich, Switzerland

Milorad Kilibarda, PhD, University of Belgrade, Faculty of Transport and Traffic Engineering

Robert Mikac, PhD, University of Zagreb, Faculty of Political Sciences

Denis Čaleta, PhD, Faculty of state and European studies, Institute for Corporate Security Studies, Ljubljana

Nenad Putnik, PhD, University of Belgrade, Faculty of Security Studies

Božidar Otašević, PhD, University of Criminal Investigation and Police Studies, Belgrade

CONTENT

TO AI OR NOT TO AI – THAT IS NOT THE QUESTION ANY MORE,
Vladan Devedzić, PhD, University of Belgrade, Faculty of Organizational Sciences, Serbian Academy of Sciences and Arts 8

PART 1: SECURITY RELATED ISSUES OF IMPLEMENTING AI IN CRITICAL INFRASTRUCTURE SYSTEMS 9

ARTIFICIAL INTELLIGENCE IN SUPPORT OF THE RISK ASSESSMENT FOR CRITICAL ENTITIES,
Alessandro Lazari, PhD, Centre for Interdisciplinary Research on Security and Resilience of Critical Infrastructure, Department of Engineering for Innovation, University of Salento - Lecce – Italy 10

THE ROLE OF ARTIFICIAL INTELLIGENCE IN DETECTING AND MITIGATING SECURITY THREATS,
Ranka Stanković, PhD University of Belgrade, Faculty of Mining and Geology 12

DECISION-MAKING IN CONDITIONS OF UNCERTAINTY TO MEET THE CHALLENGES OF NEW TECHNOLOGIES,
Zoran Keković, PhD, Belgrade University, Faculty of Security Studies 14

THE AI-CYBER THREAT LANDSCAPE: GEOPOLITICAL DYNAMICS AND EMERGING CHALLENGES,
Gil Baram, PhD, Center for Long-Term Cybersecurity and the Berkeley Risk and Security Lab, University of California Berkeley 15

CYBER SECURITY RISKS IN THE DIGITIZATION OF WATER RESOURCE MANAGEMENT,
Nikola Milivojević, PhD, Jaroslav Černi Water Institute, Belgrade, Serbia, Vladimir Milivojević, PhD, Jaroslav Černi Water Institute, Belgrade, Serbia, Boban Stojanović, PhD, University of Kragujevac, Faculty of Science, Kragujevac, Serbia, Vladimir Bačanin, Vodena, Kragujevac, Serbia 16

IMPROVEMENT AND ENHANCEMENT OF THE AIRPORT SECURITY AND SAFETY WITH AI,
Tomislav Tuntev, PhD, TAV Macedonia, Gjorgi Alcheski, PhD, TAV Macedonia 17

ARTIFICIAL INTELLIGENCE AND CYBER SECURITY: POSSIBILITIES AND RISKS,
Ana Kovačević, PhD Facultyb of Security Studies, University of Belgrade, Dragana Nikolić, PhD Institute of Nuclear Sciences Vinča, University of Belgrade 18

ARTIFICIAL INTELLIGENCE IN NUCLEAR INDUSTRY: POSSIBILITIES, CONSTRAINTS AND PATH FORWARD,
Dragana Nikolić, PhD Institute of Nuclear Sciences Vinča, University of Belgrade,
Ana Kovačević, PhD Faculty of Security Studies, University of Belgrade 19

ARTIFICIAL INTELLIGENCE AS A CRITICAL INFRASTRUCTURE, PRINCIPLES AND REDUCTION OF CYBER RISK,
Branko Primetica, Cedars International d.o.o.
egional USAID's Cyber Security Protection and Response" Program 21

PART 2: THE FUTURE OF SMART INFRASTRUCTURE SYSTEMS 23

TOWARDS A SECURE COMPUTING CONTINUUM (IOT, EDGE, CLOUD AND DATASPACES),
Luigi Romano, PhD, Computer Engineering
University of Naples "Parthenope", Naples, Italy 24

FUSION OF MACHINE LEARNING AND METAHEURISTICS FOR PRACTICAL INFRASTRUCTURE SECURITY SOLUTIONS,
Nebojša Bačanin-Džakula, PhD, Singidunum University, Belgrade 26

A REVIEW OF DYRESE SYSTEM RESULTS FOR AI DYNAMIC RESILIENCE ASSESSMENT, *Milan Stojković, PhD,*
Institute for Artificial Intelligence Research and Development of Serbia, Novi Sad, Serbia 28

AI DRIVEN SUPPLY CHAINS, *Dejan Mirčetić, PhD, Institute for Artificial Intelligence Research and Development of Serbia, Novi Sad, Serbia* 29

PART 3: LEGAL, ETHICAL AND SOCIAL ASPECTS AND IMPLICATIONS OF AI IN INFRASTRUCTURE 31

THE ROLE OF ARTIFICIAL INTELLIGENCE IN DETECTING AND SUPPRESSING CRIMINAL OFFENCES AGAINST CRITICAL INFRASTRUCTURE IN THE ENERGY AND TRANSPORT FIELDS,
Velimir Rakočević, PhD, University of Montenegro, Faculty of Law 32

THE PRESENT AND THE FUTURE OF REGULATING LIABILITY FOR DAMAGE CAUSED BY THE MOVEMENT OF AUTONOMOUS VEHICLES,
Vladimir Savković, PhD, University of Montenegro, Faculty of Law 33

THINKING OUTSIDE THE BOX: AI – ETHICAL AND LEGAL ISSUES
Miloš Knežević, PhD, University of Montenegro, Faculty of Civil Engineering 34

ROME CALL AND ALGORITHMIC ETHICS: GUIDELINES FOR THE RESPONSIBLE DEVELOPMENT OF ARTIFICIAL INTELLIGENCE

Sanja Grbović, PhD, University of Montenegro, Faculty of Law..........................35

THE ETHICAL USE OF GENERATIVE ARTIFICIAL INTELLIGENCE - REAL POSSIBILITY OR UTOPIAN CONCEPT,
Ljubomir Kljajić, Attorney at Law (Patent and trade mark,
expert in the ethical use of AI and regulations)..36

PART 4: ENHANCING INFRASTRUCTURE RESILIENCE THROUGH COLLABORATIVE APPROACHES TO AI INTEGRATION..........................37

ARTIFICIAL INTELLIGENCE AND BIOMEDICAL SCIENCE - CHALLENGES AND RISKS,
Elizabeta Ristanović, PhD, University of Defence, Belgrade...............................38

SMARTMINER PROJECT AS A ROADMAP TO SMART, GREEN AND SUSTAINABLE MINING MACHINERY WORKPLACES,
Vesna Spasojević Brkić, PhD, University of Belgrade,
Faculty of Mechanical Engineering...39

ARTIFICIAL INTELLIGENCE FROM THE PERSPECTIVE OF STANDARDIZATION,
Goran Bajić, M.Sc. in Electrical Engineering,
Institute for Standardization of Serbia
Ivan Babić, M.Sc. in Electrical Engineering,
Institute for Standardization of Serbia..41

APPLICATION OF MACHINE LEARNING TO IMPROVEMENT OF HAIL SUPPRESSION SYSTEM
Aleksandar Zečević, PhD, University of Belgrade, Faculty of Physics,
Dragana Vujović, PhD, University of Belgrade, Faculty of Physics.....................42

DATA PROTECTION IN THE ERA OF ARTIFICIAL INTELLIGENCE (AI),
Mile Šikman, PhD, University of Banja Luka,
Faculty of Security Studies and Law Faculty...44

THE ROLE OF ARTIFICIAL INTELLIGENCE IN LIGHT OF THE UPCOMING IMPLEMENTATION OF THE NIS2 DIRECTIVE
Branislav Dobrosavljević, ACS/Advanced Cyber Security...................................45

PERCEPTION OF SECURITY AND PRIVACY IN TOURIST AREAS AND THE APPLICATION OF ARTIFICIAL INTELLIGENCE
Nevena Keković, PhD Candidate, University of Split, Faculty of Economics.......46

PREFACE

Critical Infrastructure Systems (CIS) are the backbone of modern society, spanning a wide range of sectors including energy, transportation, water supply, telecommunications, security, healthcare, finance, etc. These systems are of vital importance for the functioning of economies, the well-being of citizens, as well as the efficient functioning of state bodies. They are interconnected and interdependent, which means that the disruption of even one system or part of it can have cascading and devastating effects in other systems and in society. With the increased complexity and integration of CIS, the security risks and challenges increase because most of today's critical infrastructures are based on cyber-physical systems, which means that they contain both physical and virtual aspects based on technological solutions. This structure exposes critical systems to the risks of natural disasters, cyber-attacks, physical attacks and other disasters that can have devastating consequences. Ensuring CIS security begins with identifying threats that exploit the various vulnerabilities of these systems. This requires constant investment in infrastructure maintenance, modernization and security measures, as well as cooperation between governments, private sector entities, scientific institutions, and civil society organizations.

An additional challenge is the communication within and between different systems. Two-way communication can have advantages such as faster response times, but it is also subject to additional security concerns such as loss of control over intelligent systems, especially in the face of threats from multiple sources or resulting from the interdependence of multiple sector vulnerabilities. The variety of system types, as well as the types of attacks that can cause them, require more comprehensive techniques that are able to detect threats of a different nature. These comprehensive detection methods must rely on artificial intelligence to accurately identify and classify threats under conditions of uncertainty and the need for rapid response.

On the other hand, Artificial Intelligence (AI) is a rapidly developing area in the technology industry. The importance of AI stems from its transformative potential in multiple domains, such as CIS. AI's prominent role in the CIS (energy, transport, banking, financial instrument markets, health, water, wastewater, digital infrastructure, public administration, space, food processing and distribution), lies in its ability to drive innovation, improve efficiency and solving complex challenges in different domains, ultimately shaping the future of our economy and society. In other words, the integration of AI into CIS has the potential to improve the resilience, security and efficiency of infrastructure systems, ensuring the continued functioning of essential services on which social stability relies. Many researchers and developers are widely applying methods and techniques that simulate human-like intelligence in CIS algorithmic operations.

The potential benefits of using AI in CIS are undeniable, but careful planning, development and implementation of these solutions is necessary to minimize risks and ensure responsible use of this powerful technology. One of the biggest problems is the lack of theoretical knowledge in this area. Most studies show the impressive results of the new methods without explaining in detail how they are further generalized in the face of future unforeseeable challenges. This lack of transparency and analysis of strategic risks has reduced people's confidence in new approaches. Moreover, it has made it difficult to apply appropriate international and national regulations, as well as regulation techniques as an integral part of the application of AI methods to any real-world application. The exponential development and integration of AI into all aspects of technology has also raised ideological and ethical dilemmas. Reports highlight that reliance on AI could create new system vulnerabilities that could be maliciously exploited. In short, as our world becomes increasingly interconnected and technology-driven, protecting vital infrastructure from emerging threats and improving its efficiency through AI-based solutions has become imperative.

The CRITICAL INFRASTRUCTURE SYSTEMS IN THE AI ERA (CI-AI Nexus) Conference is dedicated to exploring the symbiotic relationship between CIS and AI, and is poised to unravel the complexities and potentials of the convergence of these two transformative domains. It serves as a dynamic platform suported by Ministry of Science, Technological Development and Innovation of the Republic of Serbia for interdisciplinary dialogue, cooperation and knowledge exchange. Thanks to the partner’s support of the institutions from the academic community of Serbia and the wider region, the business community and state authorities, the researchers, engineers, policy makers, industry leaders, practitioners and investors have been actively participating in shaping the future of critical infrastructure

resilience and sustainability through the innovative integration of AI technologies.

Book of abstracts containts key topics and objectives of the Conference reflected through keynotes, thought-provoking panels, interactive workshops and presentations of the latest research, aiming to foster a deeper understanding of how AI can revolutionize the management, protection and resilience of critical infrastructure systems. Distinguished academics, scholars, researchers and practicioners were invited to explore new methodology approaches, share best practices, and chart a path to a more secure, efficient, and responsive infrastructure in an ever more challenging geopolitical and security environment. It is presented through the four chapters:

1) **Security related issues of implementing AI in critical infrastructure systems;**
2) **The future of smart infrastructure systems;**
3) **Legal, ethical and social aspects and implications of AI in infrastructure;**
4) **Enhancing infrastructure resilience through collaborative approaches to AI integration.**

President of the Scientific Board

Zoran Keković, PhD,
University of Belgrade,
Faculty of Security Studies

Vladan Devedzić, PhD, University of Belgrade, Faculty of Organizational Sciences, Serbian Academy of Sciences and Arts[1)]

TO AI OR NOT TO AI – THAT IS NOT THE QUESTION ANY MORE

Everybody's doing AI today (or at least they say so). The spectrum of AI stakeholders spans virtually all domains, and ranges from researchers, developers and companies, to educational institutions, educators and their students, to all kinds of end users, organizations, decision makers, government bodies, to society at large. Along with the undeniable and rapid growth of the stakeholder base, there is also an unwanted growth of threats and risks that misuse and abuse of AI technology in practice pose to all stakeholders. Some of them call for prompt legal regulation, and some of them represent direct perils for critical infrastructure. Worse still, due to current advances in AI, modern warfare also develops beyond all boundaries that could have been foreseen just a couple of years ago.

In this context, questions arise like: How much does AI cost? How much *could* AI cost our society? How many qualified AI professionals are there? What is the way to keep up with all AI developments worldwide? Is all that we see or seem but a dream within a dream?

Key words: Artificial Intelligence, threats, risks, critical infrastructure, legal regulation

[1)] devedzic@gmail.co

PART 1: SECURITY RELATED ISSUES OF IMPLEMENTING AI IN CRITICAL INFRASTRUCTURE SYSTEMS

Alessandro Lazari, PhD, Centre for Interdisciplinary Research on Security and Resilience of Critical Infrastructure, Department of Engineering for Innovation, University of Salento - Lecce – Italy[2)]

ARTIFICIAL INTELLIGENCE IN SUPPORT OF THE RISK ASSESSMENT FOR CRITICAL ENTITIES

As critical infrastructures become increasingly complex and interconnected, they face evolving threats from both physical and cyber domains (and beyond e.g. hybrid threats). Effective risk assessment is crucial for protecting these entities, ensuring their resilience, and maintaining essential services. Traditional risk assessment methodologies often struggle to cope with the dynamic nature of threats and the vast amount of data required for accurate analysis, leading also to the unsustainability of certain aspects of security programmes. Artificial Intelligence (AI) offers effective potential in enhancing risk assessment processes by providing advanced analytical capabilities, real-time data processing, and predictive insights.

This speech explores the application of AI technologies in supporting the risk assessment of critical entities, focusing on AI-driven methodologies that enhance the identification, analysis, and mitigation of risks. AI can process vast datasets from diverse sources, including sensor networks, cyber security systems, and public data, to detect anomalies, predict potential threats, and assess vulnerabilities with a level of speed and accuracy unattainable by human analysis alone. By leveraging machine learning algorithms, natural language processing, and advanced analytics, AI systems can dynamically adapt to new information and evolving threat landscapes, offering a proactive approach to risk management.

Key areas of AI application discussed include predictive modeling for threat anticipation (including digital twins), anomaly detection in real-time data streams, and decision support systems that assist human operators in prioritizing and responding to risks. The integration of AI into risk assessment frameworks can also facilitate scenario analysis and simulation, enabling critical entities to test the effectiveness of different mitigation strategies under various conditions. Furthermore, the use of AI enhances the ability to continuously monitor risk levels, allowing for agile adjustments to security postures in response to emergingthreats.

[2)] alessandro.lazari@unisalento.it

The speech will also brieflyaddresses the challenges and considerations in implementing AI for risk assessment, such as data quality, algorithmic transparency, and the need for human oversight to prevent over-reliance on automated systems. The ethical implications of AI use, particularly in terms of privacy and the potential for bias in decision-making, are also examined to ensure responsible deployment of these technologies.

Key words**:** risk, resilience, critical entities, Artificial Intelligence

Ranka Stanković, PhD University of Belgrade, Faculty of Mining and Geology[3)]

THE ROLE OF ARTIFICIAL INTELLIGENCE IN DETECTING AND MITIGATING SECURITY THREATS

Artificial Intelligence (AI) can analyze vast amounts of data in real-time, recognizing patterns and keywords that indicate potential threats. We will focus on the role of language technologies, from threat detection and automated threat response to prevention through multilingual threat analysis, enhanced data analysis and mitigation of attack consequences using NLP Tools. Monitoring of social media, forums, and other communication channels for discussions can detect content related to cyber threats or suspicious activities, enabling early detection of risks. Further, AI systems equipped with language technologies can automatically respond to threats by interpreting and generating human-like responses. This includes automatic generation of warnings or alerts in multiple languages, or even engaging in real-time communication with potential attackers to delay or deflect threats while security measures are implemented. The future threats can be predicted by analyzing multilingual datasets, including communications in various languages, enabling proactive protective measures from potential attacks, regardless of the language used by the attackers.

Various NLP resources and technologies for detection of security threats can be used and combined. Sentiment and emotion analysis identifies negative or suspicious sentiment in communications, emotions expressed in text, such as anger, fear, or hostility, which could be indicators of potential security threats, while topic modeling helps to identify communications related to specific security concerns (e.g., discussions about hacking, phishing). Named Entity Recognition (NER) identifies and classifies entities such as people, organizations, locations, and products in text data, helping in detection mentions of specific individuals or groups that pose security threats. The relevant keyword and phrase extraction from large datasets to highlight potential security threats is useful for monitoring social media, forums, and other online platforms for specific security-related terms.

The machine translation enables the analysis of multilingual communications based on multilingual embeddings and cross-lingual transfer learning techniques, crucial for global threat detection, as threats may be discussed in different

[3)] ranka.stankovic@rgf.bg.ac.rs

languages. The large pre-trained and fine-tuned language models can predict the continuation of a suspicious conversation or to generate alerts based on incomplete data. Social media monitoring tools track and analyze conversations on social media platforms, helping to identify and respond to emerging threats in real-time. Spam and Phishing Detection filters and flags suspicious emails or messages use pattern recognition and contextual analysis of email content.

These NLP resources and technologies, when integrated into security systems, enhance the ability to detect and mitigate security threats across different media and languages.

Key words: NLP, language technologies, language models, security threats, threat detection

Zoran Keković, PhD, Belgrade University, Faculty of Security Studies[4)]

DECISION-MAKING IN CONDITIONS OF UNCERTAINTY TO MEET THE CHALLENGES OF NEW TECHNOLOGIES

Both in practice and in the literature on crisis management, there is an established opinion that crisis planning is one of the key tasks of crisis managers and a prerequisite for the successful resolution of situations that we call crisis. The thesis that adapting plans and procedures to new situations is the key to decision-making in conditions of uncertainty is often advocated.

The goal of the work is to shift the focus of research practice and crisis management from crisis planning to the development of human resources and their ability, competence and psychological characteristics that enable their quick transition from routine to non-routine conditions. That is why we believe that professional selection and development of human resources important for decision-making in crisis situations will play a crucial role. This goes hand in hand with the development of new technologies and the possibility of applying artificial intelligence tools during the psychological profiling of the desirable characteristics of an individual as a decision maker. But even such technological implications will face the question of what is considered as an confirmed crisis manager, since the metric of results when it comes to successful decision-making in a crisis contradicts the very nature of the crisis whose long-term effects are complex and unfathomable and escape the rational criteria set by science.

Critical infrastructures as systems of systems further complicate and multiply the consequences of crisis decision-making.

Key words: Decision making, New technologies, Crisis management, Critical infrastructures, Human resources

[4)] zorankekovic@yahoo.com

Gil Baram, PhD, Center for Long-Term Cybersecurity **and the** Berkeley Risk and Security Lab**, University of California Berkeley**[5)]

THE AI-CYBER THREAT LANDSCAPE: GEOPOLITICAL DYNAMICS AND EMERGING CHALLENGES

Artificial Intelligence (AI) has emerged as a transformative force in cybersecurity, simultaneously bolstering defensive capabilities and equipping malicious actors with sophisticated attack vectors. This presentation examines the current trends and challenges in the AI-driven cyber threat landscape, addressing both geopolitical implications and evolving AI-enabled cybercrime tactics.

The integration of AI in cybersecurity operations presents a dual-edged sword, offering unprecedented opportunities for threat detection and response while also introducing new risks. This necessitates a nuanced approach that harnesses AI's potential while mitigating associated threats.

In the geopolitical arena, AI-powered cybersecurity has become a strategic asset, with nation-states competing for technological supremacy. State-sponsored groups are leveraging AI to enhance cyber operations, refine tactics, and execute more sophisticated attacks. This technological arms race raises concerns about potential escalation in cyber conflicts and underscores the need for international cooperation and regulatory frameworks.

On the cybercrime front, AI has empowered attackers with tools to craft more convincing social engineering campaigns, develop evasive malware, and improve targeting precision. Of particular concern are AI-generated phishing attacks and deepfake media, which exploit human vulnerabilities and challenge conventional security measures.

As the AI-cyber threat landscape rapidly evolves, impacting both nations and organizations, it is imperative for stakeholders across sectors to remain vigilant and adaptable. The future of cybersecurity will likely be characterized by an intricate dance between increasingly sophisticated AI-driven attacks and equally advanced AI-powered defenses. This presentation will explore strategies for navigating this complex terrain, emphasizing the importance of collaborative efforts in developing robust, AI-informed cybersecurity postures.

Key words: Cybersecurity; Artificial Intelligence; geopolitics; cybercrime

[5)] glbaram@gmail.com

Nikola Milivojević, PhD, Jaroslav Černi Water Institute, Belgrade, Serbia[6)]
Vladimir Milivojević, PhD, Jaroslav Černi Water Institute, Belgrade, Serbia
Boban Stojanović, PhD, University of Kragujevac, Faculty of Science, Kragujevac, Serbia
Vladimir Bačanin, Vodena, Kragujevac, Serbia

CYBER SECURITY RISKS IN THE DIGITIZATION OF WATER RESOURCE MANAGEMENT

The digital transformation of the water industry is revolutionizing resource management, operational efficiency, resilience, and cost optimization through the integration of advanced technologies such as the Internet of Things (IoT), Geographic Information Systems (GIS), real-time monitoring systems, automation, and Artificial Intelligence (AI). However, this increased reliance on interconnected digital platforms significantly amplifies the sector's vulnerability to cyber security threats. This paper provides a detailed examination of the critical vulnerabilities arising from the digitization of water infrastructure, with particular emphasis on the ICT aspects that are key to identifying and mitigating these vulnerabilities.

Keywords: water management, cyber security, SCADA, GIS, real-time systems.

[6)] nikola.milivojevic@jcerni.rs

Tomislav Tuntev, PhD, TAV Macedonia[7)]
Gjorgi Alcheski, PhD, TAV Macedonia[8)]

IMPROVEMENT AND ENHANCEMENT OF THE AIRPORT SECURITY AND SAFETY WITH AI

Economic growth, globalization and technical improvements have had a major impact on the airline industry. As opportunities grow and the interest of civilization changes, people are increasingly venturing into travel and visiting new unknown places. Aviation is growing rapidly, and this is generating huge benefits for the world. According to the analysis and forecasts by the Airports Council International (ACI), by the end of 2024, global airport passenger traffic is expected to reach 9.7 billion, surpassing the level of 2019 for the first time since the COVID-19 pandemic. Global airport passenger traffic is expected to exceed 20 billion in 2043, double the 2024 projection. These figures mean a great success for the industry, but also a huge responsibility for airports and airlines. Because of the high security risks, there must be strict regulations for passengers, staff and aircraft as well. As the number of passengers travelling through airports continues to increase and so do the risks, the role of Artificial Intelligence (AI) is becoming increasingly crucial. With AI systems, airports can effectively handle growing passenger volumes and deal with the associated challenges. AI in airports is revolutionizing the aviation industry by using advanced technologies to improve safety, security, efficiency and the passenger experience. This paper summarizes the role of AI at airports and how it improves operational efficiency, enhances safety and security, and provides new passenger experiences. AI enables intelligent decision making, personalized experiences and cost savings due to optimized resource planning. Finally, the paper includes the challenges and considerations, and how they should be handled, as well as the future AI trends and innovations.

Key words**:** Artificial Intelligence, aviation industry, airport, safety, security

[7)] t.tuntev@yahoo.com
[8)] gjorgi.alceski@tav.aero

Ana Kovačević, PhD Faculty of Security Studies, University of Belgrade[9)]
Dragana Nikolić, PhD Institute of Nuclear Sciences Vinča, University of Belgrade[10)]

ARTIFICIAL INTELLIGENCE AND CYBER SECURITY: POSSIBILITIES AND RISKS[11)]

Artificial Intelligence (AI), especially Machine Learning (ML), has become widespread. At the same time, cyber security attacks are increasing in number, sophistication, severity, and financial impact. Mitigating these attacks is crucial in sensitive environments, such as critical infrastructure, particularly in sectors like the nuclear industry, where the consequences of such attacks can be devastating.

Machine Learning has proven effective in analyzing large datasets and identifying patterns that were previously unknown or not obvious but useful. In this way, ML can be utilized to detect cyber attacks and block attackers. However, it can also be exploited in attacks on targeted systems, analyzing system infiltration and uncovering software vulnerabilities. Additionally, in adversarial attacks on machine learning models, the weaknesses of ML systems and their reliance on data are explored. Adversarial attacks on ML models can involve malicious manipulation of input data to deceive the models and cause incorrect decisions, potentially leading to unsafe operational outcomes in the nuclear facilities. For example, attackers could introduce small perturbations to operational data, causing the ML algorithm to incorrectly assess the system's stability. Ultimately, these attacks could compromise the safety, security, and reliability of the system, with potentially devastating consequences if not properly mitigated. Therefore, machine learning algorithms intended to secure a system must be resilient themselves. Research on adversarial attacks and defense mechanisms for ML algorithms used in the nuclear facilities is limited, highlighting the need for continued study in this area.

Key words: Artificial Intelligence, machine learning, cyber security, adversarial attack

[9)] kana@fb.bg.ac.rs
[10)] anikol@vinca.rs
[11)] The work was supported by the Science Fund of the Republic of Serbia within the framework of the 'IDEAS' Program – Management of New Security Risks Research and Simulation Development, NEWSiMR&D, #7749151

Dragana Nikolić, PhD Institute of Nuclear Sciences Vinča, University of Belgrade[12)]
Ana Kovačević, PhD Faculty of Security Studies, University of Belgrade[13)]

ARTIFICIAL INTELLIGENCE IN NUCLEAR INDUSTRY: POSSIBILITIES, CONSTRAINTS AND PATH FORWARD[14)]

The rise of Artificial Intelligence (AI) technology in recent decade has presented new opportunities and challenges for improving the safety, reliability & economic competitiveness of nuclear industry, primarily of Nuclear Power Plants (NPPs). NPP is inherently complex critical infrastructure, a dynamic system-of-systems with highly nonlinear performance, which encompasses both physical and cyber domains. It is technically challenging, multidisciplinary task to maintain capability, reliability and robustness of numerous Structures, Systems & Components (SSCs), especially of those operating in harsh environmental conditions with hazardous materials, present in the primary reactor circuit. Requirements for the nuclear safety and the nuclear security of NPP are extensive, pending very strict regulations and licence condition. Accordingly, continuous monitoring of the various systems/parameters is performed to ensure NPP is operated within the operational limits and conditions defined to prevent situations that could lead to anticipated operational occurrences or accident conditions, and to mitigate eventual consequences of such events. As a result, very large amounts of data are generated, which could be processed by AI techniques to rapidly and more accurately extract vital information about actual plant state, or to predict its behaviour.

Research studies on the implementation of AI techniques for various processes in NPP include design optimization of reactor core & radiation shielding, thermal-hydraulic simulation, main safety parameters monitoring & trend prediction, as well as online sensor calibration and fault classification. Machine learning algorithms have been employed efficiently for optimization of nuclear fuel management in the Light Water Reactor (LWR), while the ant colony algorithm was used for design optimization of radial fuel lattice of LWR. However, there are issues to be resolved before AI can eventually be implemented as an industrial grade technique for “real-world NPPs` problems”.

[12)] anikol@vinca.rs
[13)] kana@fb.bg.ac.rs
[14)] The work was supported by the Science Fund of the Republic of Serbia within the framework of the 'IDEAS' Program – Management of New Security Risks Research and Simulation Development, NEWSiMR&D, #7749151

One concern is the lack of adequate databases for training & testing AI models, especially for transients and accident scenarios. Additionally, black box nature of AI is not suitable for application in nuclear industry where criteria are very high for safety systems and functions. Further research is necessary to improve interpretability, reliability and robustness and to develop the transparency of AI models.

The cyber security aspects of the possible AI applications, particularly of Machine Learning (ML) utilization, are also discussed. It is important to analyze both the new vulnerabilities that the use of ML might introduce into the system and the ability of ML to actually detect cyber attack on a particular system. Adversarial attacks on ML models involve malicious manipulation of input data to deceive ML models and induce wrong decision, potentially leading to unsafe operational decisions in the facility. In that manner, attackers could introduce minor perturbations to operational data causing the ML algorithm to incorrectly assess stability of the considered system of a NPP. Ultimately, these attacks could undermine the safety, security, and reliability of NPP, with potentially devastating consequences if not properly mitigated. Therefore, ML algorithms intended to secure a system need to be resilient themselves. Studies on adversarial attacks and defence mechanisms on ML algorithms that are implemented in a nuclear facility are rare, so continued research is indicated.

Key words: Artificial Intelligence, nuclear reactor, machine learning, adversarial attack

Branko Primetica, Cedars International d.o.o. Regional USAID's Cyber Security Protection and Response" Program[15)]

ARTIFICIAL INTELLIGENCE AS A CRITICAL INFRASTRUCTURE, PRINCIPLES AND REDUCTION OF CYBER RISK

Artificial Intelligence (AI) will play a significant role in maintaining the reliability, evolution and performance of the critical infrastructure systems. In this regard, AI is critical to ensuring that the success of a system's performance can adapt to variances without service disruptions to the end customer. We can already see AI being used to enable better healthcare, create smart cities, improve energy management, and support remote control and automation. There is a distinct difference between how legacy technology has been used to date, and how the power of AI is being harnessed to power tomorrow's solutions. In the examples given above, AI's role is not limited to being an enabling technology solution to automate or digitize business processes. Instead, it effectively acts as the backbone of a modern infrastructure, warranting the same level of protection and strategic importance as physical and cyber domains. This presentation:

- Compares the characteristics of AI against those of critical infrastructure systems;
- Reviews potential threats and vulnerabilities when applying AI to the Critical Infrastructure Protection;
- Summarizes risks and threats to using AI in critical infrastructure;
- Cites best practices in successfully deploying defense mechanisms to protect AI solutions in critical infrastructure;
- Examines the role of governance to manage the fast pace of AI development;
- Provides a high-level case study from a confidential electricity utility.

If we are to use and define AI as critical infrastructure, we must commit to its all-encompassing development, including cyber security aspects. As with other critical infrastructure systems, AI's integrity, resilience, and reliability would be essential for the well-being of our citizens and nation.

***Key words*:** Artificial Intelligence, critical infrastructure, modern infrastructure, risk management, cyber defense, governance

[15)] branko.primetica@cedars.rs

PART 2: THE FUTURE OF SMART INFRASTRUCTURE SYSTEMS

Luigi Romano, PhD, Computer Engineering University of Naples "Parthenope", Naples, Italy[16)]

TOWARDS A SECURE COMPUTING CONTINUUM (IOT, EDGE, CLOUD AND DATASPACES)

This talk proposes a best effort approach for extending/adapting the paradigm of Trusted Computing (TC) to the new context of Computing Continuum (CC) and suggests that this concept be implemented in a flexible framework of composable services, tools and techniques. The mechanisms made available by TC in traditional computing environments enable the setup of a Trusted Computing Base (TCB) – i.e. the set of hardware, firmware, and software components of a system that are considered trusted – which is virtually vulnerability free, and can thus be used as the (initial) building block of a secure distributed computing infrastructure. The enabling factor of TC in a complex, multi-domain and multi-device environment, is that all participating entities are equipped with hardware resources which implement a set of agreed upon features (e.g. Trusted Boot, Sealed Storage, Curtained Memory, Attestation, Integrity Measurement, and Secure I/O). Obviously enough, this is typically not the case in the CC, which is characterised by: i) the co-existence of computing nodes of a highly heterogeneous nature with different computing capacity (and security support features); ii) the evolution of deployment setups according to highly dynamic and possibly autonomous mechanisms, and iii) the strong dependency on interoperable Data Spaces for correct/efficient operation. Nevertheless, it is key for the real take up of the CC paradigm that – despite these limitations and obstacles – users (from data owners to data providers) be provided with a flexible toolset for achieving the maximum level of security which is possible, given the available resources and the existing constraints.

Four categories of devices are targeted, which collectively cover the high-variety of computing nodes found in real world CC field deployments, namely:

- WTEE (With a TEE) - Devices equipped with a COTS Trusted Execution Environment technology integrated in the CPU (e.g. Intel SGX and TDX, AMD SEV, ARM TrustZone and CCA). This is typically the case of server nodes and powerful edge nodes.

[16)] luigi.romano@uniparthenope.it

- WTPM (With a TPM) - Devices equipped with a Trusted Platform Module, external to the CPU.
- WSE (With a SE) - Devices equipped with a Secure Element. This is typically the case of smartphones, tablets, and hardware crypto-wallets.
- WN (With Nothing) - Devices with no resources/features specifically dedicated to security improvement.

Examples of concrete applications of the proposed approach will be presented, with respect to substantial use cases from research projects.

Key words: Security, Computing Continuum, Trusted Computing Base

Nebojša Bačanin-Džakula, PhD, Singidunum University, Belgrade[17)]

FUSION OF MACHINE LEARNING AND METAHEURISTICS FOR PRACTICAL INFRASTRUCTURE SECURITY SOLUTIONS

Critical Infrastructure (CI) refers to physical and logical systems that are essential for the basic functioning of the economy and government. This includes things such as telecommunications, energy, banking and finance, transportation, water systems, and emergency services, both public and private. One of the major concerns in the CI is cyber security, driven by the exponential growth of security threats both online and within organizations. A key issue is the challenge of detecting intrusions and distinguishing between malicious and normal network traffic. Although a wide range of Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) is available today, they often suffer from misclassification issues, where the system can fail to recognize an attack as a threat or to mark normal traffic as malicious. Therefore, to address this rising issue Artificial Intelligence (AI) methods and algorithms could be utilized. Machine Learning (ML) and Deep Learning (DL), as subfields of AI, play an increasingly vital role in cyber security, helping to detect, prevent and respond to a variety of cyber threats against the CI. Its ability to analyze vast amounts of data, identify patterns, and make decisions in real time makes it a powerful tool for enhancing cyber security defenses, especially through integration with IPSs. However, according to the No Free Lunch theorem (NFL), universal ML and DL models, that could be successfully applied to address cyber security issues for all CI, do not exist. Each model should be tuned and adapted for specific dataset (network traffic features). This problem in literature is known as the hyper-parameter tuning and it is Non-deterministic Polynomial hard (NP-hard) in nature.

Due to the infinite number of possible hyper-parameters' values, traditional deterministic algorithms are not able to tune the models for specific tasks and utilization of metaheuristics is necessary. Therefore, the aim of this panel lecture is to introduce hybrid methods between ML/DL and metaheuristics for addressing cyber security challenges in the CI, which is a current research area in modern literature. Through practical case studies, published in scientific papers, several ML and DL models optimized by metaheuristics for tackling this problem on real-world datasets will be presented. Additionally, relatively recently adopted state-of-

[17)] mailto:nbacanin@singidunum.ac.rs

the-art DL models such as Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs) will also be exhibited along with combination of traditional ML and DL approaches.

Key words: critical infrastructure, machine learning, deep learning, metaheuristics, hybrid AI, intrusion detection

Milan Stojković, PhD, Institute for Artificial Intelligence Research and Development of Serbia, Novi Sad, Serbia[18)]

A REVIEW OF DYRESE SYSTEM RESULTS FOR AI DYNAMIC RESILIENCE ASSESSMENT

This review examines the Dyrese system's results for assessing dynamic resilience in rural and urban water systems under hazardous events. The Dyrese system integrates Artificial Intelligence (AI) techniques, particularly Artificial Neural Networks (ANNs), to estimate dynamic resilience by analyzing the impact of various hazards, including severe floods, earthquakes, and climate change effects, on water systems. The dynamic resilience assessment considers both the intensity and frequency of these events, capturing the adaptive capacity and recovery time of the systems. Using generated datasets ranging from mild to severe conditions, the ANN model assesses resilience metrics, validated through case studies such as the Pirot water system in Serbia and urban water systems in London, UK (Stojković et al. 2024; Stojković et al. 2023). These studies incorporate diverse models, including climate, hydrological, and system dynamics models, to evaluate resilience comprehensively. The review highlights how Environmental Dynamic Resilience (EDR) and Environmental Reliability (ER) provide a robust framework for understanding the sustainability and adaptive capacity of water systems in response to climatic shifts and extreme events, advancing the field of AI-driven risk management in water resource planning and resilience assessment.

Key words**:** Resilience, AI, hazards, water, adaptation

[18)] mailto: milan.stojkovic@ivi.ac.rs

Dejan Mirčetić, PhD, Institute for Artificial Intelligence Research and Development of Serbia, Novi Sad, Serbia[19)]

AI DRIVEN SUPPLY CHAINS

AI is set to transform supply chains by addressing the growing complexity of logistics processes and the increasing volume of the data generated across various touchpoints. Companies face mounting pressure to enhance supply chain planning and performance in the face of rising uncertainty and competition. Traditional approaches are no longer adequate, leading to a need for AI-driven solutions that can handle vast and diverse data sources. AI-driven supply chains can analyze vast and diverse data sources, enabling better planning, forecasting, and operational efficiency. Moreover, leveraging AI in supply chains offers a transformative potential for improving decision-making, responsiveness and driving efficiency across global supply networks.

Keywords: AI-driven supply chains, supply chain optimization, logistics automation, demand forecasting, operational efficiency.

[19)] mailto:dejan.mircetic@ivi.ac.rs

PART 3: LEGAL, ETHICAL AND SOCIAL ASPECTS AND IMPLICATIONS OF AI IN INFRASTRUCTURE

Velimir Rakočević, PhD, University of Montenegro, Faculty of Law[20)]

THE ROLE OF ARTIFICIAL INTELLIGENCE IN DETECTING AND SUPPRESSING CRIMINAL OFFENCES AGAINST CRITICAL INFRASTRUCTURE IN THE ENERGY AND TRANSPORT FIELDS

The subject of research in this paper is the role of artificial intelligence in the suppression of criminal offences against energy and traffic critical infrastructure. The goal of the research includes explanation of the contribution of artificial intelligence to crime control, determination of the scope and dynamics of incriminations, analysis of the national legal framework and its comparison with European standards, and systematization of knowledge in this area for the purpose of successful crime control. Therefore, it is the duty of official structures to effectively oppose all criminal activities that result in the destruction or damage of critical infrastructure. On the other hand, the use of artificial intelligence through the accelerated development of high technologies increasingly affects the prevention and suppression of the most serious forms of crime. These forms of criminal behavior include diversion from the group of criminal offences against the constitutional order and security of the state, which includes demolition and burning or, in other ways, the destruction or damage of critical infrastructure facilities that are of great importance for the safety and supply of citizens or for the economy and the functioning of public services with the intention of endangering the vital values of the state. Application of artificial intelligence is possible in all stages of detection and suppression of this criminal offence and by all official actors of the criminal procedure. Here, I am primarily referring to the police, who are the first to find out about a prepared or committed criminal act, then the state prosecutor's office, which manages reconnaissance and investigation, the courts that pass judgments on the perpetrators of criminal acts, the authorities responsible for the execution of court decisions, et cetera. The research will use the methodology of legal and related sciences with an emphasis on the qualitative and developmental dimension. The expected results of the research are contained in the concretization of the application of artificial intelligence in all phases of detection and suppression of the criminal offence in question in the practice of intelligence services and criminal proceedings with a focus on collecting, sorting and processing a large amount of information. The conclusion is that the fight against crime cannot be effective if artificial intelligence units such as biometric technologies, video surveillance et cetera are not used, and that a large amount of information obtained through artificial intelligence enables the competent authorities to anticipate and prevent criminal activities.

Key words: Critical infrastructure, artificial intelligence, crime, detection, suppression

[20)] mailto:veljorakocevic@yahoo.com

Vladimir Savković, PhD, University of Montenegro, Faculty of Law[21)]

THE PRESENT AND THE FUTURE OF REGULATING LIABILITY FOR DAMAGE CAUSED BY THE MOVEMENT OF AUTONOMOUS VEHICLES

In the recent years, the world is witnessing intensive scientific research and corresponding commercialization attempts in the field of automation of automobiles and other motor vehicles. It is reported that the so-called “highly automated driving vehicles” (these are considered as “level three” vehicles on the *de facto* universal five level categorization scale of autonomous vehicles) are being intensively tested and prepared for commercial use by number of manufacturers. Their key feature is allowing designated drivers to completely turn their attention away from the road under certain conditions whilst remaining prepared to take over the full control of vehicle in a matter of seconds, if need be. Hence, it seems that artificially intelligent computer programs could soon become fully responsible for our road safety, as well as for the road safety of other traffic participants. This raises some very interesting questions on both ethical and legal level. Among the most important ones is the issue of liability for damage in situations where the collision or other traffic incident involving autonomous vehicle occurred while the vehicle was fully under the control of artificially intelligent computer program. There are those arguing that the traditional rules on liability in road traffic accidents can be applied in these situations, too, meaning that there is no need for the legislative intervention. However, there are those that see things differently (for instance, particularly in situations where the injured party is the driver of autonomous vehicle himself and the accident took place while the car was in self-driving mode), meaning that they see the need for the changes of the existing regulatory frameworks. The forthcoming corresponding paper will aim to investigate the legitimacy of the latter standpoint, as well as to present the latest regulatory responses on it, although few are available at this point. Its aim would be to raise the right questions rather than to offer definitive answer and regulatory solutions.

Key words: Autonomous vehicles, ”damage”, ”liability”, regulatory framework

[21)] vsavkovic@t-com.me

Miloš Knežević, PhD, University of Montenegro, Faculty of Civil Engineering[22)]

THINKING OUTSIDE THE BOX: AI – ETHICAL AND LEGAL ISSUES

Legal science intertwines with our lives and must adapt to technological advancements. Thinking outside the box in the context of artificial intelligence (AI) is becoming increasingly significant in modern society, especially considering the ethical and legal issues accompanying its development and application. AI, as one of today's most dynamic technologies, promises revolutionary changes in various fields, from governance systems to autonomous vehicles. However, these advancements come with substantial challenges that require thinking beyond traditional frameworks. This is particularly true for the ethical dilemmas and legal regulations that need to keep pace with the rapid development of AI. One of the key ethical issues related to AI is the question of bias in algorithms. The algorithms driving AI systems often reflect the biases present in the data they are trained on. This can result in discriminatory decision-making, such as in hiring, lending, or even judicial rulings. Therefore, a comprehensive approach is needed, involving out-of-the-box thinking to identify and eliminate these biases. This includes interdisciplinary collaboration among AI experts, sociologists, legal professionals, and ethicists. On the other hand, the legal issues arising from the application of AI also require innovative thinking. Existing legal norms are often not tailored to the specifics of AI technologies. For example, the question of liability in the case of an error by an autonomous vehicle or a medical robot is not clearly defined. Is the manufacturer, the programmer, or the user responsible? Such questions necessitate new legal frameworks and regulations that effectively address the specifics of AI. Furthermore, the issue of data privacy is of utmost importance. AI systems often use vast amounts of data to function efficiently, which opens the door to potential misuse and privacy violations. Thinking outside the box can help create innovative solutions that balance the benefits of AI with user privacy protection. Therefore, thinking outside the box is not just a desire but a necessity in the context of AI development and application. Ethics and law must evolve alongside technology to ensure that its development serves society and individuals rather than harming them. Interdisciplinary collaboration, innovative approaches, and proactive regulation are key elements in addressing the ethical and legal challenges of AI. In this way, we can ensure that the benefits of AI are maximized while minimizing risks and negative consequences.

Key words: Artificial Intelligence (AI), Ethical, Legal, Bias, Privacy

[22)] knezevicmilos@hotmail.com

Sanja Grbović, PhD, University of Montenegro, Faculty of Law[23)]

ROME CALL AND ALGORITHMIC ETHICS: GUIDELINES FOR THE RESPONSIBLE DEVELOPMENT OF ARTIFICIAL INTELLIGENCE[24)]

This paper aims to highlight the importance of applying ethical standards in the development and use of artificial intelligence, with a special focus on the 'Rome Call', one of the key documents that provides ethical guidelines for the future development of this technology.

In February 2020, the Pontifical Academy for Life and the RenAIssance Foundation signed the Rome Call for Ethical Development of Artificial Intelligence (Rome Call). Pointing to a new "algorithic", more precisely "algorithmic ethics", the signatories pledged to advocate for the development of artificial intelligence that will serve each individual and humanity as a whole, that will respect the dignity of the human person, ensuring justice and transparency, responsibility and respect for human rights, so that every individual can benefit from the future technological progress.

Furthermore, the Rome Call includes three main areas of influence: ethics, education and rights, as well as six principles on the basis of which it carries out its activities, namely: transparency, inclusivity, responsibility, impartiality, reliability, security and privacy.

In the concluding remarks, the author emphasizes that the adoption of regulations to standardize the provision of artificial intelligence services, along with ensuring a high level of reliability and security for these systems, will be crucial tasks for all states in the future.

***Key words**:* Artificial Intelligence, Rome Call , ”Algor - Ethics”, security and data protection.

[23)] sanjag @ucg.ac.me

[24)] Founded on April 12, 2021 by Pope Francis, the RenAIssance Foundation is a non-profit organization that aims to promote anthropological and ethical reflection on the effects of new technologies on human life.

Ljubomir Kljajić, Attorney at Law (Patent and trade mark, expert in the ethical use of AI and regulations)[25)]

THE ETHICAL USE OF GENERATIVE ARTIFICIAL INTELLIGENCE - REAL POSSIBILITY OR UTOPIAN CONCEPT

Artificial intelligence, through the breakthrough of tools based on generative artificial intelligence models (such as ChatGPT), has gained significant public attention, and rightly so. In the past two years, the use of generative artificial intelligence tools has brought about significant changes in society in the fields of work, business, creativity, and other social aspects, whose impact will only be measurable or observable in, not so not-so-distant future. Some of these changes include massive job losses, accelerated process automation, and the penetration of "artificial creativity" into society, with which society is currently struggling to maintain balance by introducing restrictive legal frameworks.

As the first societal response to the phenomenon of "artificial intelligence," prior to a flux of legislative initiatives, the question of the ethical use of artificial intelligence emerged. In March 2023, the Republic of Serbia adopted *the Ethical guidelines for the development, implementation and use of robust and accountable AI* on the level or recommendations, to lay the foundation for robust and accountable artificial intelligence.

The fundamental requirement of the *Ethical Guidelines* is that artificial intelligence systems that are developed or applied must be in accordance with the well-being of humans, animals, and the environment. In principle, robust and accountable artificial intelligence is: technically robust and safe, transparent, and where accountability can be established in accordance with the law and established ethical principles and values.

Keywords: Ethical use of Artificial Intelligence, bias, transparency, safety, robustness, accountability.

[25)] ljubomirkljajic@gmail.com

PART 4: ENHANCING INFRASTRUCTURE RESILIENCE THROUGH COLLABORATIVE APPROACHES TO AI INTEGRATION

Elizabeta Ristanović, PhD, University of Defence, Belgrade[26]

ARTIFICIAL INTELLIGENCE AND BIOMEDICAL SCIENCE - CHALLENGES AND RISKS

Artificial Intelligence (AI) is gaining more and more space in our lives every day, and the question arises whether we will soon control it or it will control us? The COVID-19 pandemic has shown that AI has significantly improved our ability to monitor, predict and respond to such complex health crises as outbreaks (spread assessment, trajectory tracking, diagnostic tools development, drug and vaccine discovery assistance, big data processing, optimizing of resources management, simplifying of administrative procedures etc) as well as the use of robots in diagnostics, treatment, conducting of operative and surgical procedures, patient monitoring, prognostic and predictive modeling, information placement etc. The potential use and benefits of AI in neurosciences, surgery and other fields of medicine are practically unlimited, but at the same time it is opening a new Pandora's box of its possible abuse, because healthcare today in the era of hybrid wars could be also considered as a security challenge, and cyber security and bio-security are inseparable segments of the modern integrative approach to security issues. Healthcare, as a complex and dynamic field, requires precision, efficiency and constant innovation. The use of AI is very useful tool for that as well as for decision makers and effective medical management and leadership. However, it opens numerous ethical and security dilemmas, some of which have already been raised and discussed during the pandemic itself. The need for effective legal and other regulation and security protection of medical and genetic data and biodiversity is an imperative of the present moment and an issue of major geopolitical battles that are currently taking place in the sphere of genetics, biotechnology and the pharmaceutical industry between the People's Republic of China and the USA, while other actors such as the Russian Federation proclaimed the genetic sovereignty and data protection. All mentioned political powers and the other subjects in the dynamically changing world as well other developed countries has been permanently working on the broad use of AI in the progress of medical science with the great potential for its potential abuse. Thus, the real question for experts and decision-makers today is how to find the real balance in this field in the triangle science progress – security – ethics? All these questions will be discussed in the paper.

Key words: AI, healthcare, outbreaks, data protection, biotechnology.

[26] elizabeta.ristanovic@vma.mod.gov.rs

Vesna Spasojević Brkić, PhD, University of Belgrade, Faculty of Mechanical Engineering[27)]

SMARTMINER PROJECT AS A ROADMAP TO SMART, GREEN AND SUSTAINABLE MINING MACHINERY WORKPLACES[28)]

Recent publications have acknowledged the many difficulties, concerns, and problems facing the mining industry, as one of the oldest industries, still encountered today, all of which require immediate attention. Through the SmartMiner project, we are driven to suggest a variety of green digital transformation strategies and solutions. By aligning advanced operator I4.0&5.0 and society S5.0 standards, project proposes novel concept which contains smart solutions for raising the level of environmental quality in complex interactions between physical, behavioral, and organizational processes field. It also proposes a paradigm shift from pure technology to a Human and Data-Centric Engineering, which can be easily transferred to other industries. Namely, mining machinery operator and his environment represent a set of complex interactions between physical, psychosocial, and organizational factors and processes, which, if mastered could lead to sustainable company performance and people-centric smarter society. SmartMiner approach points out to operator's workplace micro and macro environment. Operator's MICRO environment is represented by his physical environment – noise, human vibration, lighting, temperature, air quality, workplace layout etc. Job stressors load, if sustained over time, produces adverse effects such as health and safety problems and lack of performance. Operator's MACRO environment is determined by organizational contextual factors – safety awareness, competence and communication on operational and managerial level, organizational environment dimensions, management support, risk judgment and management reaction, safety precautions, accident prevention. Micro and micro levels as physical processes layers are to be connected and balanced by real time analytics – digital processes layers to fit high sustainability performance indicators (economic, social, environmental etc.). After data collection on operators (460) and managers (160) in surface mines, the structural equational modelling and multicriteria decision aid methodologies are applied.

[27)] vspasojevic@mas.bg.ac.rs

[28)] This research was supported by the Science Fund of the Republic of Serbia, #GRANT No. 5151, Support Systems for Smart, Ergonomic and Sustainable Mining Machinery Workplaces – SmartMiner and the Ministry of Science, Technological Development and Innovation of the RS according to the Agreement on financing the scientific research work of teaching staff at accredited higher education institutions in 2024, no. 451-03-65/2024-03/200105 from 05.02.2024.

Continuous monitoring and data acquisition on noise, whole body vibrations, thermal stress, humidity, emission of gaseous and particulate pollutants from internal combustion engines, and indoor air quality (gases, particulate pollutants) at operator’s workplace through sensors, is also done. Finally, using the machine learning tools and algorithms, the predictive optimization models will be developed in aim to predict the level of each workplace pollution and safety parameters and productivity assessment, in line with innovative context-specific multi-sensorial mining machinery operator aid system, based on sensorial model and sustained with the soft/management parameters measurement scales, in aim to enable improvement and optimization of techno-economic, environmental and societal aspects of a workplace, while maintaining the highest standards of safety.

***Keywords**:* Mining machinery, operator, smart, green, sustainability

Goran Bajić, M.Sc. in Electrical Engineering, Institute for Standardization of Serbia[29)]
Ivan Babić, M.Sc. in Electrical Engineering, Institute for Standardization of Serbia, Institute for Standardization of Serbia[30)]

ARTIFICIAL INTELLIGENCE FROM THE PERSPECTIVE OF STANDARDIZATION

As AI technologies advance, the need for standardized frameworks to ensure their safe, ethical, and effective deployment becomes increasingly critical. Standardization in AI aims to establish common guidelines and practices that promote interoperability, reliability, and trustworthiness of AI systems. ISO/IEC JTC 1/SC 42 committee, has been working on AI standards since 2018.
Key areas of AI standardization include:

– Terminology and Definitions: Establishing a common language for AI to ensure clear communication among stakeholders.

– Data Management: Guidelines for data collection, processing, and protection to maintain data integrity and privacy.

– System Performance: Standards for evaluating the performance, accuracy, and reliability of AI systems.

– Ethical and Trustworthy AI: Frameworks to ensure AI systems are developed and used ethically, addressing issues like bias, transparency, and accountability.

The standardization process involves collaboration among governments, industry, academia, and other stakeholders to address the diverse challenges posed by AI.

In conclusion, standardization in AI is essential for fostering a trustworthy and sustainable AI ecosystem. By establishing clear guidelines and best practices, standardization efforts aim to mitigate risks, enhance interoperability, and promote the responsible development and deployment of AI technologies.

***Key words**:* Standardization, interoperability, ethics, reliability, trustworthiness

[29)] goran.bajic@iss.rs
[30)] ivan.babic@iss.rs

Aleksandar Zečević, PhD, University of Belgrade, Faculty of Physics[31]
Dragana Vujović, PhD, University of Belgrade, Faculty of Physics[32]

APPLICATION OF MACHINE LEARNING TO IMPROVEMENT OF HAIL SUPPRESSION SYSTEM

Large hailstones cause considerable economic losses, especially in agriculture and infrastructure. In order to mitigate the consequence of the hail precipitation, hail suppression has been practised in Serbia since 1967. The main goal is to reduce the size or frequency of hailstones. Cloud seeding is carried out in certain areas of the cloud, which are determined by a specific isotherm height and radar reflectivity. We would like to answer the following question: Could the process of hail suppression be improved if the prediction of the heights of the specific isotherms and the values of radar reflectivity obtained by the numerical weather prediction model is improved with the machine and deep learning algorithms? Therefore, the goal is to improve the forecast of the vertical temperature profile and reflectivity field through the application of various machine and deep learning algorithms.

Machine learning algorithms such as linear regression, random forests, decision trees and gradient boosting were used. In addition, neural networks (in the first order sequential model) and U-NET convolutional neural network can perform well in the downscaling process due to the prompt setting of the model architecture. Based on the modelled temperature values at 15 isobar levels, we want to obtain a more detailed vertical profile containing 91 values in the interval from 1000 to 100 mb, which better represents the current state of the atmosphere observed by sounding than a linear interpolation. In order to better predict the direction of the storm movement as well as critical values of the radar reflectivity (e.g. those greater than 45 dBz), the challenge is to use spatio-temporal neural networks that would take as input a time series with a resolution of 15 minutes, three fields represented in a 2D matrix and the reflectivity field, the satellite image of the water vapour channel (WV 6.2 μm) and the surface value of the temperature. In this way, the reagent containing silver iodide would be introduced and released in a more precisely defined area and the critical infrastructure could be better protected.

[31] zecevic050@gmail.com
[32] dvujovic@ff.bg.ac.rs

For the training of the above machine and deep learning models, the data of the vertical profile of the forecast temperature of the ECMWF Integrated Forecasting System (IFS) model with a resolution of 0.125 × 0.125 degrees for 6h, 12h, 18h and 24h ahead on 15 vertical isobar levels, as well as radiosonde measurements over Belgrade, representing the observed real state, were used. For radar reflectivity, EUMETSAT channel_5 data, composite radar reflectivity and ECMWF forecast of surface temperature over the area of interest were used.

The gradient boosting regressor, which uses only the temperatures from the model as independent variables to calculate the temperatures at 91 isobaric levels, performed best with mean squared error of 1.367. In comparison, the linear interpolation of the air temperatures from the model levels to 91 isobaric values from 1000 to 100 mb has a larger mean squared error of 1.94.

Keywords: Hail suppression, machine learning algorithms, vertical temperature profile, radiosonde, radar reflectivity, the gradient boosting regressor

Mile Šikman, PhD, University of Banja Luka, Faculty of Security Studies and Law Faculty[33)]

DATA PROTECTION IN THE ERA OF ARTIFICIAL INTELLIGENCE (AI)

Data in the era of Artificial Intelligence (AI) is a very valuable resource, because without data even AI would not have the capabilities it has today (collection, processing and analysis of data). We are especially referring to personal data that their holders "selflessly" share and make available to a wide range of interested parties. The data available in this way is increasingly being manipulated and misused for criminal purposes, which threatens the guaranteed rights and freedoms of citizens multiple times. Therefore, the question of data protection in the era of AI is raised as an imperative. In addition to other forms of protection (e.g. copyright protection, patent protection), criminal law protection stands out, the purpose of which is to suppress and prevent behavior that misuses the personal data of citizens. The aim of the work is to review the existing criminal law norms that provide protection to personal data in the context of their abuse through AI and to provide concrete proposals for the improvement of this area.

Keywords: Data, protection, artificial intelligence, AI, Criminal law

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

Branislav Dobrosavljević, ACS/Advanced Cyber Security[34)]

THE ROLE OF ARTIFICIAL INTELLIGENCE IN LIGHT OF THE UPCOMING IMPLEMENTATION OF THE NIS2 DIRECTIVE

The start of the implementation of the new NIS2 directive in the EU is a hot topic of all expert meetings, both from the narrower field of cyber security, and from the broader perspective of business risk management as an essential element of sustainable development. The obligation of the member states was to harmonize their legislation with this directive by October 17, 2024, while full implementation in the EU is expected in the period 2026/2027. During the preparations for the implementation of the NIS2 directive in the EU countries many questions were opened at the level of national legislation, Directive implementators and providers of future solutions.

The NIS2 directive poses special challenges to the candidate countries of the Western Balkans, which are not EU members but are economically and politically closely tied to it, and the provisions of the NIS2 directive will apply to many of their subjects. In this study, starting from the specifics of Serbia and our region, we tried to single out several of the most important issues, and to offer possible solutions for some of them. Our analysis of a wide range of sources showed that, of the many issues observed at the EU level, the issue that stends out is availability of quality solutions for cyber security to small and medium-sized enterprises (SMEs), many of which will be to some extent covered by the application of the NIS2 directive and local laws harmonized with it.

This study presents ACS ARMADA, existing modern SIEM platform solution in Serbia and associated Security Operations Center (SOC). The specifics of this SIEM solution are easy and fast implementation and integration, flexible commercial models, adaptability to special user requirements and easy scalability. This solution is accompanied by a comprehensive set of Blue and Red Team services, and is rounded off by the engagement of partner SME firms and top individual consultants as needed.

The manufacturer's lean, economical business model, accompanied with ever increasing applliccation of AI/ML, will allow ACS ARMADA SIEM platform and accompanying services to be far more achievable to SMEs than comparable vendor solutions.

Key words: NIS2 Directive; SIEM; ACS ARMADA; SMEs; Solution achievability.

[34)] branislav.dobrosavljevic@acs.co.rs

Nevena Keković, PhD Candidate, University of Split, Faculty of Economics[35)]

PERCEPTION OF SECURITY AND PRIVACY IN TOURIST AREAS AND THE APPLICATION OF ARTIFICIAL INTELLIGENCE

In an era of rapid progress in the use of artificial intelligence across numerous and nearly all sectors of the economy and social life, it is essential to further examine this phenomenon from the perspective of its application in tourism. This issue can be viewed from the perspective of tourism supply, where artificial intelligence can provide significant support, or from the perspective of demand, where there is often public discontent on social media regarding AI technologies. Additionally, the question of the application and awareness of existing tools to which both supply and demand are exposed daily arises.

When considered within the framework of security (of destinations, users, or data), this becomes particularly significant given the unique characteristics of security aspects at tourist destinations and the specific security challenges that destinations, tourism supply, and demand face. In this sense, artificial intelligence can be viewed from two angles – from the perspective of supporting security measures and from the perspective of potential risks to users during its application. This paper reflects on the perception of supply and demand within a specific tourist area, investigating visitors' trust, with an emphasis on data protection and privacy concerns, as well as the understanding and trust of supply representatives in the potential of these technologies.

The research was conducted in tourist areas in Montenegro. Treating tourism as one of the primary economic sectors in Montenegro, and considering security as a serious challenge, whether related to cyber security or the safety of people and property, this research can provide substantial support for the future application of artificial intelligence technology in the field of security.

The methodology used includes a combination of quantitative and qualitative techniques. Data was collected through surveys of tourists to assess their awareness of AI applications and their attitudes towards security and privacy. Additionally, interviews were conducted with managers of tourism facilities to

[35)] nevena.kekovic@gmail.com

gain insights into the practical aspects of AI implementation and their perception of the potential risks or benefits these technologies bring to the tourism sector.

The final results of the research will indicate the level of awareness, information, perception, and trust in artificial intelligence tools among supply representatives, but primarily among demand representatives, i.e., tourists. The results of this research could be a valuable support for policymakers in the fields of tourism and security, as well as for all stakeholders in the tourism market.

Key words: Artificial Intelligence, tourist market, perception of security, trust, privacy

CIP - Каталогизација у публикацији
Народна библиотека Србије, Београд

005.334:351.759.6(048)
005.334:61(048)

INTERNATIONAL SCIENTIFIC AND EXPERT CONFERENCE (2024)

Conference Book of Abstracts / INTERNATIONAL SCIENTIFIC AND EXPERT CONFERENCE:
CRITICAL INFRASTRUCTURE SYSTEMS IN THE ERA OF ARTIFICIAL INTELLIGENCE [and] CIS-AI NEXUS – CONVERGENCE IN CRITICAL INFRASTRUCTURE AND ARTIFICIAL INTELLIGENCE,

17-18 October, 2024 ; [editor Zoran Keković]. - Belgrade: Center for Risk Analysis and Crisis Management, 2024 (Novi Beograd: Data Copy). - 47 str. ; 24 cm

Tiraž 100. - Str. 5-7: Preface / Zoran Keković.

ISBN 978-86-902810-7-7

а)Ванредне ситуације -- Безбедност – Апстракти

б)Управљање ризиком -- Безбедносни сектор – Апстракти

в)Кризни менаџмент – Апстракти

г)Вештачка интелигенција -- Примена -- Апстракти

COBISS.SR-ID 153059849

center

for risk analysis and
crisis management

ISBN 978-86-902810-7-7