



**European Institute of Further Education
School of Engineering Management
“Union – Nikola Tesla” University**

International Scientific-Professional Conference

Book of Abstracts

**ARTIFICIAL INTELLIGENCE AND
SECURITY IN THE XXI CENTURY**

Editor: Dr. Katarina Štrbac

**November 19, 2025
Belgrade**

ISBN 978-80-89926-24-4 (EIFE)

EAN 9788089926244

ISBN 978-86-89691-45-0 (SEM)

BOOK OF ABSTRACTS
International Scientific-Professional Conference
ARTIFICIAL INTELLIGENCE AND SECURITY
IN THE XXI CENTURY
November 19, 2025

Dr. Katarina Štrbac (Ed.)

Conference organiser
School of Engineering Management, “Union-Nikola Tesla” University,
Belgrade, Republic of Serbia

Podhájska and Belgrade, 2025.

ARTIFICIAL INTELLIGENCE AND SECURITY IN THE XXI CENTURY

BOOK OF ABSTRACTS

International Scientific-Professional Conference

ARTIFICIAL INTELLIGENCE AND SECURITY IN THE XXI CENTURY

November 19, 2025

Organisation

School of Engineering Management, "Union-Nikola Tesla" University, Belgrade, Republic of Serbia

Publisher

European Institute of Further Education, Slovakia
School of Engineering Management, "Union-Nikola Tesla" University, Serbia

For the Publisher

Dr. Jozef Zat'ko
Professor Dr. Vladimír Tomašević

Editor

Dr. Katarina Štrbac

Cover Design & Layout

Dr. Katarina Štrbac

Print

Black & White
Number of copies: 100

ISBN 978-80-89926-24-4 (EIFE)

EAN 9788089926244

ISBN 978-86-89691-45-0 (SEM)

© 2025 European Institute of Further Education, Slovakia and School of Engineering Management, "Union-Nikola Tesla" University, Serbia

Editor: Dr. Katarina Štrbac

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License (CC BY-NC-ND 4.0).

DOI: https://doi.org/10.65690/sem_ais21a.2025

Disclaimer: The opinions represented in this publication do not represent the official positions of the organizations in which its authors hold employment, nor do they represent the positions of the publishers of this Conference Proceedings, its editors, or its sponsoring organizations.

ARTIFICIAL INTELLIGENCE AND SECURITY IN THE XXI CENTURY

SCIENTIFIC COMMITTEE

President

Dr. Vladimir Tomašević, Full Professor, Dean, School of Engineering Management, “Union-Nikola Tesla” University, Belgrade, Serbia

Distinguished Members

Dr. Vanja Rokvić, Associate Professor, Faculty of Security, University of Belgrade, Serbia

Dr. Vera Arežina, Associate Professor, Faculty of Political Sciences, Belgrade, Serbia

Dr.h.c. mult. JUDr. Jozef Zat’ko, PhD, DBA, European Institute of Continuing Education, Pothajska, Slovakia

Dr. Octavian Buiu, Scientific Director, National R&D Institute for Microtechnologies and Associate Professor at the National University for Science and Technology Politehnica Bucharest, Romania

Dr. Francisco Rubio Damián, Associate Professor, Universidad San Jorge, Zaragoza, Spain

Dr. Javier Porras Belarra, Senior Lecturer, Spanish National Distance Education University – UNED (Ministry of Education), Madrid, Spain

Dr. Nahla Hamdan, Full Professor, American University in the Emirates, UAE

Dr. Renata Petrevska Nechkoska, Associate Professor, University St. Kliment Ohridski Bitola, N. Macedonia, part of European University Alliance COLOURS; Ghent University Belgium

Dr. Tetiana Bukoros, Associate Professor, National University of
Ukraine, Kyiv, Ukraine

Dr. Nenad Komazec, Associate Professor, University of Defence,
Serbia

Dr. Eldar Saljic, Full Professor, American University in the Emirates,
UAE

Dr. Aleksandar Ivanov, Full Professor, Faculty of Security, Skopje,
North Macedonia

Dr. Branislav Milosavljević, Associate Professor, Faculty of
Business and Law, "Union – Nikola Tesla" University, Belgrade, Serbia

Dr. Ivan Dimitrijević, Assistant Professor, Faculty of Security,
University of Belgrade, Serbia

CONFERENCE ORGANISERS

Dr. Katarina Štrbac, Full Professor, School of Engineering Management, “Union-Nikola Tesla” University, Belgrade, Serbia

Dr. Ana Jurčić, Associate Professor, School of Engineering Management, “Union-Nikola Tesla” University, Belgrade, Serbia

Dr. Milena Cvjetković, Associate Professor, School of Engineering Management, “Union-Nikola Tesla” University, Belgrade, Serbia

Dr. Damir Ilić, Assistant Professor, School of Engineering Management, “Union-Nikola Tesla” University, Belgrade, Serbia

MSc Luka Latinović, Teaching Fellow, School of Engineering Management, “Union-Nikola Tesla” University, Belgrade, Serbia

MSc Olga Mašić, Teaching Assistant, School of Engineering Management, “Union-Nikola Tesla” University, Belgrade, Serbia

PREFACE

Artificial Intelligence (AI) is fundamentally transforming the paradigm of contemporary security, opening unprecedented possibilities while simultaneously creating new and complex threats. The International Scientific-Professional Conference "Artificial Intelligence and Security in the XXI Century," held on November 19, 2025, at the School of Engineering Management, "Union-Nikola Tesla" University, brings together experts from the fields of security, technology, law, and ethics to examine the multidimensional impact of AI on national and international security in the 21st century. This gathering represents a crucial intersection where academic rigor meets practical urgency, where theoretical frameworks encounter real-world challenges, and where diverse perspectives converge to address one of the most consequential transformations of our era. The conference explores key areas of AI application in the security sector, including predictive threat analytics, autonomous defence systems, intelligence data processing, and biometric identification, examining how AI is reshaping the very foundations of security operations—from enhancing situational awareness and accelerating decision-making processes to enabling capabilities that were unimaginable just a decade ago. Particular attention is devoted to the growing cyber threats that AI enables and amplifies: sophisticated deepfakes and disinformation campaigns, automated and adaptive cyberattacks, information manipulation at unprecedented scale, and the complex challenges of hybrid warfare. These are not distant theoretical concerns but present realities that demand immediate attention and coordinated response. Throughout the sessions, participants analyse the profound ethical dilemmas arising from AI use in security contexts: questions surrounding autonomous weapons systems and the delegation of life-and-death decisions to algorithms, the implications of mass surveillance for democratic societies, algorithmic bias in security-related decision-making, and the delicate balance between collective security and individual privacy. These are not merely technical questions—they strike at the heart of our values, governance systems, and vision for human dignity in an algorithmically mediated world. The conference examines the current state and urgent needs for developing legal frameworks at both national and international levels, discussing the EU AI Act and its implications for security operations, UN initiatives aimed

at governing autonomous weapons and AI in warfare, and the critical necessity for global cooperation in establishing standards, norms, and accountability mechanisms that can keep pace with technological advancement. The remarkable international scope of this gathering—bringing together scholars and practitioners from sixteen countries across four continents—reflects both the global nature of AI's security implications and the universal recognition that no single nation, institution, or discipline can navigate these challenges in isolation. From theoretical foundations to practical implementations, from ethical principles to regulatory frameworks, diverse perspectives enrich collective understanding and strengthen capacity to develop effective, responsible approaches. Through panels and presentations, this conference creates a platform for substantive dialogue among policymakers, security professionals, technology industry representatives, academic researchers, and civil society organizations. The shared goal is to define a responsible approach to implementing AI in security contexts—one that maximizes benefits while minimizing risks, balances innovation with accountability, and ensures technological advancement serves rather than undermines human security and dignity. The forty presentations assembled in this Book of Abstracts represent cutting-edge research spanning eight critical thematic areas: AI regulation and ethics, military and defence applications, cybersecurity and hybrid threats, critical infrastructure protection, education and higher learning, healthcare and diagnostics, smart cities and public safety, and data privacy and protection. Each contribution reflects rigorous scholarship, practical insight, and commitment to ensuring that artificial intelligence enhances rather than compromises global security. The path forward requires thinking across traditional boundaries, questioning assumptions, balancing competing values, and collaborating across disciplines and borders. The insights shared, the relationships formed, and the frameworks developed through this conference contribute to shaping a future where artificial intelligence serves as a tool for enhancing security while preserving the values that make security worth protecting. This conference represents not merely an exchange of knowledge, but the beginning of sustained dialogue and cooperation that will guide the responsible development and deployment of AI in the security domain for years to come.

KEYNOTE SPEECH 1

Dr. Vladimir Tomašević, Full Professor, Dean, School of Engineering Management, “Union-Nikola Tesla” University, Belgrade, Serbia

Distinguished guests, esteemed colleagues, ladies and gentlemen,

It is my great honour and privilege to welcome you to the International Conference on "Artificial Intelligence and Security in the 21st Century," hosted here at the Belgrade School of Engineering Management. Today marks a significant moment in our collective journey to understand, shape, and responsibly govern one of the most transformative forces of our time— artificial intelligence. Looking around this room, and across our virtual connections, I see representatives from sixteen countries spanning four continents. We have scholars, practitioners, and policy experts who are online from Spain to Trinidad and Tobago, from Lithuania to the United Arab Emirates, from France to North Macedonia, and from many nations in between—including Belgium, Bosnia and Herzegovina, Cyprus, the Czech Republic, Germany, Montenegro, Serbia, Slovakia, and Turkey. This remarkable geographic diversity is not merely a statistic to celebrate—it represents something far more profound. It demonstrates our shared recognition that artificial intelligence transcends borders, cultures, and political systems. The challenges we face, and the opportunities we must seize, require exactly this kind of international dialogue and cooperation. Over the course of today's conference, we will explore forty cutting-edge research presentations that span the entire spectrum of AI's intersection with security. These presentations have been carefully curated to address the most pressing questions of our time, organized around eight critical thematic areas. First, we will examine AI regulation and ethics—the foundational frameworks that must guide our technological development. Our colleagues will present on everything from EU legal regulations and their security implications to the ethical dilemmas surrounding AI misuse and responsibility. We'll hear about intercultural approaches to AI ethics, exploring how we can reconcile ethical universalism with cultural diversity in an increasingly connected world.

Second, we'll delve into military and defence applications, addressing perhaps some of the most consequential questions humanity faces today. How do we govern the use of artificial intelligence for military purposes? What are the risks and management challenges of autonomous weapons systems in contemporary warfare? And fundamentally, what legal foundations must we establish for peace in the age of artificial intelligence? Third, cybersecurity and hybrid threats will

take centre stage as we examine AI's dual role—both as a tool for protection and as a vector for new forms of attack. We'll explore AI-driven phishing attacks, the amplification of hybrid threats in the Western Balkans, information manipulation through emerging technologies, and the sophisticated challenge of deepfake technology. These presentations will help us understand not just the technical dimensions of these threats, but their geopolitical and social implications. Fourth, critical infrastructure protection demands our attention. From airport security systems enhanced by AI threat detection to the protection of smart cities like Dubai, from innovative technologies securing vital installations to advanced approaches in ecological security—our presenters will demonstrate how artificial intelligence is reshaping the way we protect the essential systems upon which modern society depends. Fifth, education and higher learning will be examined through the lens of both opportunity and responsibility. How do we develop ethical and security awareness for responsible AI use? What role do large language models play in higher education, and how do we address issues of integrity and institutional policy? How can AI transform predictive modelling of student performance and governance in transnational university alliances? These questions are critical as we prepare the next generation for an AI-integrated world. Sixth, healthcare and diagnostics will reveal AI's profound impact on human life and wellbeing. We'll critically examine artificial intelligence in medical diagnostics, exploring not just its capabilities but its risks, responsibilities, and epistemological limits. This session reminds us that behind every algorithm are human lives that demand our utmost care and ethical consideration. Seventh, smart cities and public safety will showcase how artificial intelligence is transforming urban life. From consumer trust in AI-enabled marketing to the security aspects of smart city development, these presentations will help us understand how AI reshapes the spaces where most of humanity now lives. Finally, data privacy and protection will address one of the most fundamental rights in the digital age. How do we protect personal data in the context of AI? What regulatory and technological frameworks can ensure anonymization and metadata transformation? How do we prevent the leakage of sensitive technical documentation into general-purpose large language models? But our conference addresses even more than these eight themes. We'll explore the reliability and security of AI models in hardware systems, the application of machine learning in industrial safety and refinery processes, the role of AI in intelligence analysis and decision-making systems, and the economic aspects of artificial intelligence and security. We'll examine digital diplomacy in the MENA region, strengthening EU-

Morocco cooperation on AI and cybersecurity, and the geopolitical dimensions of AI's relationship with national security. What unites all forty presentations is a shared commitment to rigorous scholarship, practical application, and—most importantly—responsibility. Each presenter has grappled with difficult questions that don't have easy answers. They've conducted empirical research, developed theoretical frameworks, and proposed solutions to problems that didn't exist a decade ago. They represent the frontline of human effort to ensure that artificial intelligence serves humanity's highest aspirations rather than its darkest fears. As we gather here in Belgrade—a city with a rich history of intellectual discourse and cultural exchange—we carry forward a tradition of seeking knowledge and wisdom in times of great change. The questions we address today will shape the security landscape for generations to come. They will influence how nations interact, how societies function, and how individuals experience safety, privacy, and dignity in an increasingly AI-mediated world. I want to thank our presenters for their dedication, our organizing committee for their tireless efforts, and each of you for your participation and engagement. The conversations that begin in this conference room will continue long after today ends—in your research, in your institutions, in policy discussions, and in the practical decisions that will shape our collective future.

Let me close with this thought: artificial intelligence is neither inherently good nor inherently dangerous. It is a tool—perhaps the most powerful tool humanity has ever created—and like all tools, its impact depends entirely on the wisdom, ethics, and foresight of those who wield it. That is why your presence here today matters so much. The work you do, the questions you ask, the standards you set, and the collaborations you forge will determine whether AI becomes a force for security and human flourishing or a source of new vulnerabilities and threats.

Today, representatives from sixteen nations, bringing diverse perspectives, experiences, and expertise, have come together with a common purpose. Together, we will advance the conversation. Together, we will share knowledge. And together, we will work toward a future where artificial intelligence enhances security, respects human dignity, and serves the common good.

Thank you, and welcome to what promises to be an intellectually stimulating and profoundly important conference. Let us begin.

KEYNOTE SPEECH 2

Maja Mikić, Chief Operating Officer, AikBank, Serbia From the Vault to the Vector: A Practitioner's Framework for AI Security Governance in XXI Century Banking

The New Frontier of Trust For generations, the institution of banking has been built on the foundational principle of trust. Customers entrusted financial institutions to secure their assets in physical vaults, maintain accurate ledgers, and act as prudent stewards of their financial lives. The security of the industry was measured in the thickness of steel doors and the integrity of its people. Today, the sector is undergoing a profound transformation. Our vaults are no longer just physical; they are digital. Our most valuable assets are not just currency, but data. And our ledgers are evolving into living, learning algorithms. The industry is in the midst of a great migration—from the vault to the vector. This AI revolution promises a future of unprecedented efficiency and deeply personalized customer experiences. However, as we stand on this new frontier, we must recognize that the nature of security itself has fundamentally changed. This analysis is not merely theoretical. It is grounded in the practical experience of deploying a proprietary AI platform at AikBank to reinvent one of the most complex financial products: the home mortgage. Through this journey, a critical lesson has emerged: AI security is not an IT checklist. It is a profound challenge to our governance, our ethics, and the very definition of our fiduciary duty.

Pillar: The Algorithmic Fiduciary Duty

The first pillar of a robust AI security framework is the establishment of an Algorithmic Fiduciary Duty. A fiduciary duty represents the highest standard of care in finance, obligating an institution to act in its customers' best interests. For decades, this duty has guided human decisions. Now, it must be extended to the algorithms making decisions on our behalf. Consider a concrete example from AI-powered mortgage lending. A model could be optimized for a single variable: speed of approval. While the model would become incredibly efficient at processing applications, it might approve a loan for a family that cannot sustainably afford it. In this scenario, the algorithm succeeds on its metric, but the bank fails in its duty. The result is not just a future default, but a negative human outcome that the institution enabled. Therefore, a modern governance framework must insist that an AI's objective function is not merely profit or efficiency, but customer well-

being. This involves building in ‘ethical guardrails.’ For instance, a mortgage model should not just assess the probability of repayment; it should also simulate the customer’s financial resilience to economic shocks. This is fiduciary duty, encoded. It is the modern equivalent of a loan officer counselling a family on the long-term implications of their financial commitments.

Pillar: From Static Validation to Continuous Vigilance

The second pillar requires a shift from Static Validation to Continuous Vigilance. The traditional approach to risk management involved validating a model once, before deployment. A model would be tested, documented, and put into production under the assumption that its performance would remain stable. With AI, that assumption is not just outdated; it is dangerous. AI models are not static artifacts. They are dynamic systems that exist in a symbiotic relationship with the data they ingest. When the external world changes, the data changes, and the model’s reliability can degrade rapidly—a problem known as ‘data drift.’ An underwriting model trained on a decade of stable economic growth, for example, may become unreliable during a sudden economic crisis, as the patterns of income and employment it learned are no longer valid. To counter this, a ‘set and forget’ approach is insufficient. Financial institutions must practice continuous vigilance. This means AI security cannot be a gate; it must be a / watchtower. Automated systems should monitor the statistical properties of incoming data in real-time. When data begins to drift from the patterns the model was trained on, it should trigger an alert, summoning human experts to investigate whether the model needs to be retrained or even temporarily taken offline. This same system also serves as a first line of defence against adversarial attacks, where malicious actors attempt to ‘poison’ the data to manipulate outcomes. Continuous vigilance is the acknowledgment that in the world of AI, security is not a onetime event, but a perpetual process.

Pillar: Pragmatic Transparency and the ‘Black Box’

The third and final pillar is the need for Pragmatic Transparency. The ‘black box’ problem of AI, where the internal workings of a complex model are not easily interpretable, presents a serious challenge. For regulators, auditors, and banking leaders, this opacity is a significant concern. However, the goal should not be perfect, absolute transparency—which is often technically infeasible—but rather pragmatic transparency, tailored to the stakeholder. In practice, this means: • For

the Regulator: While a regulator may not need to understand the weighting of every neuron in a neural network, they do require assurance of a robust governance process. Institutions must be able to demonstrate data lineage, present model validation reports, provide fairness audits, and share the logs from continuous monitoring systems. The objective is to prove that the system is under control, even if its every inner working cannot be perfectly articulated. • For the Customer: When an application is denied, a customer deserves a clear, human understandable reason. Modern explainability techniques (e.g., SHAP, LIME) can translate a complex algorithmic decision into a simple, actionable explanation, such as, ‘The application was denied because the debt-to-income ratio exceeds the established guidelines.’ This approach respects the customer’s dignity, provides a path for recourse, and builds trust, even in a negative outcome. Pragmatic transparency is about providing the right level of insight to the right audience, turning the ‘black box’ into a tool of responsible communication.

Building the Guardrails for Responsible Innovation

The journey from the vault to the vector is not just a technological one; it is a cultural and ethical one. It requires the financial industry to redefine its oldest duties, build systems of perpetual vigilance, and communicate with a new kind of transparency. The three pillars of Algorithmic Fiduciary Duty, Continuous Vigilance, and Pragmatic Transparency form a framework not to slow innovation, but to enable it. They are the guardrails that allow institutions to accelerate responsibly, ensuring that the incredible power of AI is harnessed for the benefit of customers and the stability of the financial system. The challenges are immense, and no single institution has all the answers. The work being done in academic and research institutions is critical, but it must be informed by the realities of implementation in the field. A deeper collaboration between the academics who design these powerful tools and the practitioners who are tasked with deploying them safely is essential. Together, we can build a future where the promise of AI is fully realized— a future that is not only more efficient, but also more fair, more transparent, and fundamentally, more secure.

KEYNOTE SPEECH 3

Nikola Petrović, ISAC FUND Director

I would like to thank to the Belgrade School of Engineering Management, Dr. Vladimir Tomašević the Dean and professor Dr. Katarina Štrbac for the invitation to the Conference.

And as we live in the times of (so called) AI ascension, the subject of Artificial intelligence is the major topic across policies, economies and markets worldwide. And for good reason — this accelerating technology and tools are likely to produce head-spinning shifts in many aspects of life and work and it will and it already has huge impact on Security and National Security.

Ultimately the most consequential aspect of the AI revolution comes down to the cold, hard reality of security. This is clearly proven by the fact that many military planners and policymakers have likened the disruptive potential of AI to the advent of nuclear weapons 80 years ago.

Why? Well, the access and processing of Information was always a key part of any security component, from planning and policies to the actual operations and actions. And no tool has ever provided more opportunities in gathering and analysing information besides providing new avenues for disruptive actions (or attacks if you prefer) and, also, defensive actions.

This brings a question: How can governments, militaries and other security actors around the world navigate a struggle for control and use of this quickly evolving technology? Bear in mind that AI are, at least in the western world, developed by private entities unlike the last comparable information management leap – the internet, which had its root in US Department of Defence, DARPA's project for computer information network called ARPANET.

Luckily, today we have a large and representative group of experts to help us with this and many other questions regarding usage of AI's in security sphere.

I would like to just shortly present the scope of possible issues involving the ever-evolving state of AI and security

Governance and control

- **Lack of regulation:** Current governance frameworks are struggling to keep pace with the rapid development of AI, creating a dangerous gap

that weaponized AI can exploit.

- **Intensified competition:** The AI race between major powers could lead to a destabilizing competition and wide spread abuse.
- **Need for ethical frameworks:** There is a critical need for robust ethical guidelines, oversight, testing, and impact assessments to ensure AI is used responsibly in national security, along with a need for cultural change within agencies to integrate AI effectively.

Military and defence

- **Autonomous weapons and Missile defence:** AI-powered weapons systems raise ethical concerns about lethal autonomous weapons, particularly those that can select and attack targets without human control.
- **Intelligence and targeting and Advanced radar systems:** The use of AI in intelligence gathering and targeting can enhance state power but also threatens military norms.
- **Cybersecurity:** AI can enable more sophisticated cyberattacks, while national security systems using AI become vulnerable to new attack vectors, such as "data diet vulnerability".

Broader security threats

- **Misinformation and destabilization:** Adversarial actors can use AI to create sophisticated disinformation campaigns, like deepfakes, to spread false narratives, destabilize societies, and undermine democratic institutions.
- **Bioweapons:** AI could be used to accelerate and weaponize genetic engineering, potentially leading to new and more devastating bioweapons.
- **Energy security:** need to be mentioned as potential avenue but the sector that already has long tradition of autonomous systems.
- **Systemic risk:** The integration of AI across critical sectors like biotech,

cybersecurity, energy and financial systems could lead to cascading and unprecedented systemic risks and risk of domino effect.

- **Human Factor:** Many mitigating tool popularized is the human oversight and final decision making especially when it comes to critical decisions, but for such process to be even remotely possible and successful decision makers would need to be trained to work with the AI.

Societal and ethical issues

- **Bias and discrimination:** AI systems trained on historical data can perpetuate and amplify biases, leading to unfair or discriminatory outcomes in areas like predictive policing.
- **Surveillance:** The deployment of AI for government surveillance can pose a significant threat to civil liberties and privacy.
- **Transparency and accountability:** Many AI systems function as "black boxes," making it difficult to understand their decision-making processes, which is a major problem in high-stakes national security contexts where human oversight is critical.

Also, there are many security specific areas where AIs can provide both additional values and additional risks, like border management, airport security, migration management, etc., and I am sure we will have opportunity today to hear a lot more about such issues too. With that I will finish and for the end let me just remind you that AI makes attacks faster, cheaper and harder to defend against and that autonomous military systems already exist. Thank you!

KEYNOTE SPEECH 4

**Dr. Duško Tomić, Full Professor, School of Engineering Management,
"Union-Nikola Tesla" University, currently on sabbatical at American
University in the Emirates, UAE**

Entering the 21st century, the global security landscape has undergone the deepest transformation since the Cold War. Traditional models based on military power, territorial control, geopolitical balancing, and linear planning no longer provide stability, predictability, or societal resilience. The emergence of Artificial Intelligence (AI) has accelerated this shift by introducing a new form of power — algorithmic power, exercised through data processing, automated risk assessment, digital infrastructures, predictive analytics, and the management of information flows. Modern security threats are no longer confined by geography, state actors, or conventional conflict. They are transnational, networked, nonlinear, hybrid, and time-compressed. AI changes the very nature of security by enabling anticipation, behavioural modelling, automated decision-making, and simulation of scenarios that surpass human cognitive capacity. In this sense, AI is not merely a technological resource — it becomes a security paradigm, a new foundation upon which national defence strategies, cyber security architectures, border control systems, intelligence operations, and societal stability are built. States, institutions, and systems that fail to master AI risk losing the ability to protect sovereignty, infrastructure, the economy, and the social order. Theoretical Foundation:

Why Is AI Becoming a Security Paradigm?

To understand why AI is becoming the fundamental security paradigm of the 21st century, it is necessary to reflect on the shift occurring within the theoretical foundations of security and power. Classical schools of international relations — realism, liberalism, and constructivism — define power through military force, resources, institutions, norms, and identity. However, in the digital age, the central resource becomes data, while the key instrument of power becomes algorithmic processing and information governance. AI introduces the concept of algorithmic sovereignty, in which a state is not powerful because it possesses territory, but because it controls digital flows, communication channels, biometric identification, information networks, and predictive behavioural models of populations and actors. Security stops being reactive and becomes

anticipatory — instead of responding to threats, AI enables their prediction, simulation, management, and neutralization before they materialize. This transforms the ontology of security: from physical to digital, from material to informational, from hierarchical to network-based. AI is also a multiplier of other technologies — quantum systems, satellite navigation, biometrics, autonomous platforms, and cyber infrastructures. For this reason, artificial intelligence is no longer viewed as a technological addition, but as the core structural foundation of a new security reality. AI and the Redefinition of National Security Artificial Intelligence is reshaping the very architecture of national security by influencing strategic documents, operational procedures, institutional capacities, and the way critical state functions are managed. Modern states are integrating AI into national security strategies, defence doctrines, crisis management protocols, civil protection planning, and the standardization of intelligence and security processes. One of the key aspects of this transformation relates to the protection of critical infrastructure, including energy grids, airports, hospital systems, transportation hubs, telecommunications networks, food logistics, and water supplies. AI enables predictive maintenance, vulnerability identification, automated anomaly detection, and rapid incident response. In the field of border control, migration, and transnational movement, AI drives the development of biometric systems, smart video surveillance, movement pattern analytics, real-time risk assessment, and identity management. As a result, national security shifts from the physical control of territory toward the management of data, digital traces, and algorithmic profiling. Additionally, AI transforms the concept of sovereignty, as a state that does not control its digital domain loses the ability to protect its institutions, economy, population, and strategic interests. For this reason, AI becomes a strategic prerequisite for preserving the stability and resilience of modern nations. AI and Military–Security Transformation Artificial Intelligence is radically transforming military doctrine, operational capacities, and deterrence strategies by introducing a new logic of warfare based on speed, automation, and informational dominance. Traditional military platforms — tanks, aircraft, artillery — are no longer the primary source of battlefield superiority. Instead, advantage shifts to systems capable of rapidly analysing massive datasets, optimizing tactical decisions, and coordinating operations at a scale beyond human capability. Autonomous combat systems, including drones, robotic ground units, and maritime autonomous platforms, represent a new stage of force projection in which a fundamental question emerges: who authorizes the

use of lethal force — the human or the algorithm? Despite ethical dilemmas, states are rapidly developing algorithmic deterrence, based not only on weapons, but on the ability to disrupt, paralyze, or disorient adversaries through information–cyber means. Command hierarchies are being reshaped through digitalized planning systems, conflict simulations, and automated logistics networks. Warfare becomes multidimensional, where physical, cyber, space, and informational domains operate in an integrated fashion. AI ushers in an era in which advantage belongs not to the largest army, but to the actor who processes, models, and predicts the fastest — making AI a central pillar of modern military security.

AI in Intelligence and Security Structures

The intelligence sector is undergoing its deepest transformation since the advent of satellite reconnaissance and signals intelligence during the Cold War. Artificial Intelligence automates key phases of the intelligence cycle — from data collection and filtering, through analytical assessment, to predictive modelling and the generation of operational recommendations. Modern intelligence actors no longer rely solely on information but on algorithmic anticipation, meaning that systems can predict probable behaviour of individuals, organized groups, terrorist cells, criminal networks, or political actors. AI enhances all intelligence collection disciplines: OSINT through analysis of open-source digital footprints, SIGINT through intercepted communication patterns, GEOINT through satellite anomaly detection, SOCMINT through social media monitoring, CYBINT through digital infiltration and cyber tracing. Predictive profiling becomes especially significant — identifying radicalization, financial linkages, illicit flows, smuggling routes, and risks associated with violent extremist actors. This shifts the role of the analyst from a data interpreter to a strategic evaluator of algorithmic outputs, raising concerns about transparency, bias, and oversight over automated assessments. Intelligence services that fail to integrate AI become slower, reactive, and vulnerable, as adversaries — state and non-state — already use AI for concealment, deception, and operational adaptation. Therefore, AI becomes a fundamental determinant of modern intelligence superiority.

AI in the Domain of Cyber Security

Cyberspace has become the primary front of modern security challenges, and within it, AI plays a dual role — as the most powerful tool of defence and as a

sophisticated instrument of attack. Traditional cyber security systems relied on static rules and manually defined threat patterns, making them too slow and ineffective against contemporary attacks that evolve continuously. AI introduces an adaptive, autonomous, and predictive logic of cyber defence through automatic detection of zero-day attacks, anomaly identification in network behaviour, self-directed response protocols, and continuous learning based on emerging attack vectors. However, AI is equally used as a mechanism of attack: algorithmically generated phishing, bot networks for destabilization, automated intrusions into financial systems, and deepfake content employed for political destabilization, diplomatic manipulation, and the erosion of public trust. In the realm of hybrid warfare, AI enables the integration of cyber operations with psychological campaigns, economic disruptions, and information sabotage. This blurs the boundaries between war and peace, allowing attacks to be invisible, deniable, and detached from traditional military and political frameworks. For this reason, states, institutions, and the private sector must develop AI-based cyber resilience systems, because without them they remain vulnerable to attacks capable of paralyzing infrastructure, finance, healthcare, communications, and state functionality.

AI and Societal Security

Artificial Intelligence increasingly influence social cohesion, collective narratives, perception of reality, and the psychological stability of communities. In the contemporary information ecosystem, algorithms shape what citizens see, think, feel, and believe — making societal security dependent on digital infrastructure and information governance models. AI enables precise manipulation of content through personalized propaganda messaging, micro-targeting of political behaviour, polarization of public opinion, amplification of ideological divides, and creation of digital "echo chambers." Such processes can destabilize democracy, erode trust in institutions, radicalize marginalized groups, and generate social tensions that previously could not be produced with such speed or intensity. Within the framework of human security, AI affects privacy, mental autonomy, digital rights, and social equality. Algorithmic bias may reinforce discrimination based on ethnicity, gender, religion, or socio-economic status. Automated decision-making systems in healthcare, social services, and employment may create invisible mechanisms of exclusion. At the same time, AI contributes to safety by enabling early detection of criminal activities, public-

space monitoring, violence prevention, and improved emergency response. Due to this dual nature, societal security in the AI era requires a balance between technological efficiency and the protection of human rights — ensuring that digital transformation strengthens rather than undermines social stability and collective integrity.

Ethics, Law, and the Normative Architecture of AI Security

The development of AI raises complex questions related to ethics, accountability, legal oversight, and international regulation, because systems affecting security, identity, and decision-making must be transparent, fair, and normatively controlled. The central ethical question is: who bears responsibility when an algorithm makes a decision that causes harm — the programmer, the state, the user, or the technology itself? An additional challenge arises from the potential for discriminatory algorithmic models that, based on biased data, generate unequal treatment of citizens, opening the door to abuse, repression, and selective application of force. Legal and regulatory frameworks are unable to keep pace with the speed of technological change. International law, humanitarian law, and the normative standards of warfare do not anticipate autonomous combat systems, automated use of force, digital sovereignty, or algorithmic governance of populations. The European Union seeks to establish the most advanced regulatory model through the AI Act, while states such as the United States and China develop strategic approaches prioritizing power, innovation, and geopolitical competition. The normative architecture of AI must address key questions: limits of surveillance, algorithmic transparency, oversight of autonomous systems, protection of privacy, preservation of mental autonomy, data security, and mechanisms of international control. Without clear rules, AI may become an instrument of domination, repression, and destabilization — while with responsible regulation, it becomes the foundation of a secure and ethically sustainable digital civilization.

AI in the context of the UAE and the GCC

The Gulf region represents one of the most dynamic environments for the application of AI in the fields of security, economic governance, and state modernization. The UAE is among the first countries in the world to establish a national AI strategy, a specialized ministry, and an institutional framework dedicated to the digital transformation of the security sector. In the domain of

critical infrastructure, the UAE applies AI in airport security—particularly at DXB and DWC—through biometric identification systems, predictive passenger flow algorithms, automated surveillance, and intelligent risk management protocols. In the fields of border control and migration, smart control systems, digital identities, and integrated security platforms enable precise regulation of transnational movement. For GCC states, AI is essential for protecting energy networks, maritime routes, strategic infrastructure, and for responding to increasing drone and ballistic threats. Simultaneously, the region faces high exposure to information warfare campaigns, digital extremism, and geopolitical competition among major powers through technological ecosystems. AI therefore becomes both an instrument of strengthening state sovereignty and a potential source of technological dependency from external actors. This is why the UAE is developing models of domestic AI capacity building, academic programs, research centres, and partnerships with universities and security institutions — including in aviation security, intelligence studies, crisis management, and strategic security disciplines.

The Geopolitics of AI as a New Global Division of Power

Artificial Intelligence is becoming a key determinant of global geopolitics, as states no longer seek dominance over territory, resources, or trade corridors, but over digital ecosystems, technological standards, strategic data, and algorithmic infrastructures. The world is being shaped by four dominant AI blocs: the United States, China, the European Union, and Russia — each representing a distinct model of technological power and security governance. The United States leads through a corporate technological complex driven by companies such as Google, Palantir, Microsoft, and OpenAI, combining military superiority with private-sector innovation. China is developing a techno-state model of sovereignty based on population surveillance, centralized data control, and the strategic Belt and Road expansion framework. The European Union lacks military–digital dominance but seeks to impose a global regulatory standard, believing that rules can become instruments of power. Russia focuses on information and hybrid warfare, using AI to destabilize, manipulate, and infiltrate through cyber and propaganda mechanisms. AI therefore becomes a core factor in international relations, determining new alliances, economic dependencies, technological colonization, standardization, and strategic rivalry. Nations that fail to develop independent AI capabilities risk becoming peripheral digital protectorates,

making the geopolitics of AI a fundamental question of national survival.

Risks, Limitations, and Paradoxes of AI Security

Although AI brings advanced capabilities for protection, governance, and risk anticipation, it simultaneously generates new forms of insecurity, dependency, and vulnerability. The greatest paradox of AI security lies in the fact that systems designed to enhance stability may become instruments of destabilization, repression, or autonomous action beyond human control. Key risks include algorithmic bias, erosion of privacy, digital colonization through technological dependence, information manipulation, automation of violence, degradation of critical thinking, and the transfer of decision-making from humans to opaque algorithmic systems. Security infrastructures become vulnerable because they rely on complex digital networks whose disruption can trigger collapse of energy grids, medical equipment, aviation systems, financial platforms, or national communications. In the wrong hands, AI can become a tool for terrorism, criminal networks, authoritarian regimes, and irregular hybrid actors. Another paradox emerges when states adopt AI to protect citizens, yet expand surveillance over them — creating the risk of eroding freedoms, mental autonomy, and social individuality. For this reason, security in the AI era must not be viewed solely as a technical issue, but as an ethical, political, normative, and civilizational concern, because only a balance between power and responsibility can prevent the destructive consequences of technological dominance.

Future Trends in the Development of AI in the Security Sector

The future of Artificial Intelligence in the security domain will be shaped by technological, geopolitical, and societal processes that extend beyond existing capacities. Key trends include the development of quantum AI, which will dramatically increase computational power, break the strongest encryption standards, and transform cyber warfare. Neuro–algorithmic integration will enable direct interfaces between the human brain and digital systems, opening possibilities for cognitive enhancement but also for the manipulation of human consciousness. Fully autonomous security networks will manage infrastructure without human supervision, raising profound questions regarding accountability and control. Digital identity is becoming a new form of citizenship credential, where biometrics, blockchain, and AI define access to services, mobility, social rights, and interaction with the state. Algorithmic sovereignty will emerge as the

new measure of national power, since states that do not control their own data and AI models will be unable to protect institutions or citizens. In parallel, AI will transform the nature of warfare through swarm drones, autonomous command systems, and real-time information manipulation. These trends indicate that the world is entering a new stage of civilizational development — one in which security will depend not on weapons, but on the control of data, algorithms, and digital reality.

AI as the Inevitable Security Matrix of the 21st Century

Artificial Intelligence is no longer a technological innovation, but the foundational structure of modern security, power, and state governance. It impacts the military, intelligence services, cyberspace, critical infrastructure, migration management, societal stability, political processes, and international relations. States, institutions, and societies that fail to develop AI become vulnerable, dependent, and geopolitically marginalized, while those that master AI gain a strategic advantage that surpasses traditional dimensions of power. AI defines the future through three core premises: Without AI, there is no national security. Without AI, there is no sovereignty. Without AI, there is no societal stability. At the same time, the danger lies in the fact that AI can undermine privacy, autonomy, democratic processes, and human rights if balance is not established between efficiency and ethics. Therefore, it is essential that AI becomes regulated, transparent, and accountable, serving society rather than dominating it. In the 21st century, security is no longer defined by territory, military force, or economic capacity, but by the ability to manage algorithms, data, digital perception, and informational flows. AI is the new security paradigm, and understanding it becomes an intellectual, political, and strategic imperative of the modern world.

ARTIFICIAL INTELLIGENCE AND SECURITY IN THE XXI CENTURY

PANEL I: AI AND THE NEW SECURITY PARADIGM

THE SIGNIFICANCE OF ARTIFICIAL INTELLIGENCE IN NATIONAL SECURITY PROTECTION

Dejan Milenković¹, Katarina Štrbac², Jelena Mitić³

Abstract: Artificial Intelligence (AI) represents one of the keys technologically innovative tools in the domain of national security, enabling significant improvements in data processing, security threat analysis, and decision-making support. Its application in the security structures of the Republic of Serbia potentially contributes to greater efficiency and precision in preventing and detecting terrorist activities, organised crime, cyber-attacks, and other forms of security threats. It gains particular significance in the context of big data analysis, where it enables the identification of patterns and indicators of potential threats, thereby facilitating a proactive and timely response. Within special investigative measures – such as electronic surveillance, covert tracking, video surveillance, simulated transactions, controlled deliveries, and clandestine investigations – the application of AI can significantly increase efficiency and reduce operational risk. The paper analyses key areas of AI application in the context of national security, technological and institutional challenges in its implementation, as well as relevant ethical and legal aspects. The aim of the work is to highlight the importance of integrating contemporary AI solutions into existing security systems and to contribute to strategic planning of national security development in the digital age.

Keywords: national security, artificial intelligence, special investigative measures, organised crime, terrorism, cybersecurity.

¹ Ministry of Interior, Belgrade, Serbia

² School of Engineering Management, “Union-Nikola Tesla” University, Belgrade, Serbia

³ Faculty of Philology, University of Belgrade, Serbia

THE RELATIONSHIP BETWEEN ARTIFICIAL INTELLIGENCE AND NATIONAL SECURITY: GEOPOLITICAL DIMENSIONS

Branislav Milosavljević⁴, Sladjan Milosavljević⁵

Abstract: The development of Artificial Intelligence (AI) represents one of the most significant phenomena of the 21st century, profoundly altering the concepts of power, sovereignty, and security in the contemporary international system. In an era of global digitalisation and technological interdependence, states are increasingly recognising AI as a key resource for preserving national interests and projecting geopolitical influence. In the age of comprehensive global digitalisation and growing technological interconnectedness, states are acceleratively recognising AI as an essential strategic resource for maintaining and preserving vital national interests, as well as for effectively projecting geopolitical influence on the global stage. The paper analyses the relationship between AI and national security through a geopolitical lens, with particular emphasis on the role of the United States and China in shaping the new technological order. The authors examine how AI transforms the concept of security, how it is used in military, intelligence, and cyber structures, and what risks and ethical challenges it brings. The aim of the work is to argue the thesis that competition for technological leadership in the field of AI represents the central arena of contemporary international rivalry. Moreover, the competition between major powers is not merely a technological race, but has implications for establishing new global standards, rules of engagement, and economic dominance, thereby directly shaping the future of the global order and the architecture of international security.

Keywords: artificial intelligence, national security, geopolitics, digital sovereignty, global order.

⁴ Faculty of Business Studies and Law, "Union Nikola Tesla" University, Belgrade, Serbia

⁵ School of Engineering Management, "Union Nikola Tesla" University, Belgrade, Serbia

ARTIFICIAL INTELLIGENCE AND INTELLIGENCE ANALYSIS

Ivan Dimitrijević⁶

Summary: The use of Artificial Intelligence (AI) technologies is vast and widespread. The AI entered everyday life, both professional and private, and it inevitably affected the process of traditional human-led intelligence analysis. For much of a time, the intelligence analysis was based on human processing of data and on providing the insight through critical and contextual thinking. The influx of information and communication technologies (ICT) into its work facilitated processing of big data sets, but kept critical thinking on the human side of intelligence analysis. Now, the AI as a game changer in almost all life aspects should be seen as a boost for intelligence analysis not only in data collection, processing, and provision of insight, but also in the process of giving answers or directions for human analysts. However, because of some documented disadvantages of the use of AI, the full-scale use of it in the process of intelligence analysis is under big question. Not only because of morality of its use, but also because of its imperfections. Still, there is more than one example of efficient use of AI in intelligence analysis, both national and private. Here, the positive examples of its use will be presented, through a review of existing tools used by national intelligence agencies, as well as private and open-source intelligence enterprises. AI tools are integrated into the intelligence cycle and used for collection of data, processing of big data, for predictive analytics, as well as for generating summaries and reports. It is also being used for monitoring of data generated in real time which is of big value for early warning and gaining tactical advantage. All of the up-to-date and state of the art AI tools used in the intelligence analysis will be presented.

Keywords: artificial intelligence, intelligence analysis, intelligence cycle, AI tools.

⁶ Faculty of Security Studies, University of Belgrade, Belgrade, Serbia

ECONOMIC ASPECT OF ARTIFICIAL INTELLIGENCE AND SECURITY IN THE 21ST CENTURY

Pantelis Sklias⁷, Dusko Tomic⁸,

Abstract: The economic aspect of Artificial Intelligence (AI) and security in the 21st century represents a dynamic intersection of technological innovation, global competitiveness, and national resilience. AI has become a core driver of economic growth, enhancing productivity, optimizing decision-making, and transforming industries such as finance, defence, and critical infrastructure. However, this same technology introduces new vulnerabilities, including cyber threats, data breaches, and algorithmic manipulation that can undermine financial stability and national security. The integration of AI in defence economics enables states to reduce operational costs, automate intelligence processes, and predict security risks with unprecedented precision. Meanwhile, the global AI arms race has intensified economic competition among major powers, leading to strategic investments in AI-driven research, military modernization, and regulatory frameworks. The 21st-century economy is thus increasingly defined by “algorithmic security,” where data, knowledge, and computational power constitute strategic assets. Balancing innovation with ethical governance, economic sustainability, and international cooperation remains essential to harness AI’s potential while mitigating its disruptive impact on economic and security systems.

Keywords: Artificial Intelligence (AI), Security, Economy, Technological Innovation, Cybersecurity, Economic Growth, Algorithmic Security, National Resilience, Defence Economics, Global Competitiveness, Ethical Governance

⁷ Neapolis University Pafos, Cyprus

⁸ American University in the Emirates, UAE

RISKS AND MANAGEMENT OF AUTONOMOUS WEAPONS IN CONTEMPORARY WARFARE: A COMPREHENSIVE ANALYSIS

Katarina Jankovic⁹, Milica Mladenovic¹⁰, Nenad Komazec¹¹

Abstract: The rapid technological advancement in artificial intelligence (AI) has precipitated a paradigm shift in military capabilities, with autonomous weapons emerging as a critical domain of strategic and ethical concern. This research critically examines the multifaceted risks associated with the integration of autonomous weapons systems into military conflict landscapes, exploring their technological potential and inherent security challenges. The proliferation of autonomous weapons represents a complex technological innovation that transcends traditional military engagement strategies. By leveraging advanced AI technologies, these systems challenge established international security frameworks and introduce unprecedented ethical and operational uncertainties. This study conducts a comprehensive risk analysis that encompasses technological, strategic, legal, and humanitarian dimensions of autonomous weapon deployment. The research methodology employs a systematic approach to risk identification, assessment, and management. Through comprehensive literature review, expert consultations, and scenario modelling, the study investigates potential risks such as algorithmic bias, unintended escalation, accountability challenges, and the potential for autonomous systems to operate beyond human control. The analysis reveals that while autonomous weapons offer significant tactical advantages, they simultaneously introduce substantial risks to global security architectures. Key findings underscore the critical need for robust international governance mechanisms and comprehensive risk management strategies. The research proposes a multi-stakeholder framework for mitigating autonomous weapon risks, emphasizing the importance of interdisciplinary collaboration among technologists, policymakers, military strategists, and ethicists. By providing a nuanced understanding of autonomous weapon risks, this study contributes to the emerging discourse on responsible AI development in military contexts. The findings advocate for proactive risk

⁹ General Staff of the Serbian Army, Directorate for Development and Equipment J-5, Technical Test Centre, Centre for Testing Armaments and Military Equipment, Nikinci, Republic of Serbia,

¹⁰ Regional Association for Security and Crisis Management RABEK, Belgrade, Serbia,

¹¹ University of Defence, Military Academy, Belgrade, Serbia

management approaches that balance technological innovation with ethical considerations and global security imperatives.

Keywords: Risk, Risk Management, Autonomous Weapons, Artificial Intelligence, Military Technology, Global Security

GOVERNING THE USE OF ARTIFICIAL INTELLIGENCE FOR MILITARY PURPOSES

Vanja Rokvić¹²

Abstract: Artificial intelligence (AI) is increasingly transforming the character of modern warfare. At the same time, a new revolution in military affairs has given rise to growing concerns over a global AI arms race, driven by strategic competition among major powers. In response, the regulation of military applications of AI has emerged as a key issue on the international agenda. This paper analyses key initiatives addressing these challenges, with particular attention to debates within the United Nations Convention on Certain Conventional Weapons (CCW), relevant United Nations (UN) resolutions, and the positions of the International Committee of the Red Cross (ICRC). National instruments such as the U.S. Department of defence Directive 3000.09 are examined alongside non-binding frameworks including European Union guidelines, NATO strategies, and political declarations. A unifying theme across these efforts is the preservation of meaningful human control over the use of force, as well as the assurance of legal accountability, predictability, and reliability of AI-enabled military systems. The paper also analyses the advocacy of the Stop Killer Robots campaign, which has been instrumental in elevating the issue of lethal autonomous weapons systems (LAWS) and calling for a ban on systems capable of independently identifying and attacking human targets. Despite growing consensus on key principles, no binding international treaty specifically regulating AI in weapons systems currently exists. The current regulatory landscape remains at a formative stage, characterized by growing consensus on key principles such as human control and legal accountability, but divided by geopolitical interests. While initiatives within the UN and other forums signal momentum toward binding norms, significant challenges, such as verification, definitional clarity, and arms race dynamics, continue to hinder progress.

The global governance landscape remains fragmented and politically divided, underscoring the need for sustained multilateral cooperation to establish a balanced and enforceable framework for AI in warfare.

Keywords: artificial intelligence, autonomous weapons systems, lethal autonomous weapons systems, AI arms race, regulations, AI governance, AI Accountability

¹² Faculty of Security Studies, University of Belgrade, Serbia

AI'S ROLE IN AMPLIFYING HYBRID THREATS IN WESTERN BALKANS

Igor Novaković¹³, Marko Savković¹⁴

Abstract: Artificial Intelligence (AI) is increasingly shaping the security landscape of the Western Balkans, a region marked by fragile political environments and contested governance. This paper examines how AI amplifies hybrid threats such as cyberattacks, facilitates election interference, and enables destabilization by both state and non-state actors. Through machine learning and automated systems, malicious actors can create disinformation campaigns, exploit vulnerabilities in digital infrastructure, and manipulate public opinion. The study places these developments within the broader context of hybrid threats, highlighting the interplay between technological innovation and systemic weaknesses in democratic institutions. By analysing recent cases and emerging trends, the paper argues that AI-driven security challenges in the Western Balkans are not merely technical but deeply political, requiring coordinated responses that combine cybersecurity measures, regulatory frameworks, and resilience-building at societal and institutional levels.

Keywords: Artificial Intelligence (AI), Cybersecurity, Election Interference, Hybrid Threats, Disinformation Campaigns, Western Balkans, Political Stability

¹³ ISAC FUND, Belgrade, Serbia

¹⁴ ISAC FUND, Belgrade, Serbia

INFORMATION MANIPULATION AND PSYOPS VIA DIGITAL OUT-OF- HOME (DOOH) MEDIA

Liljana Pecova -Ilieska¹⁵

Abstract: Digital Out-of-Home (DOOH) media—digital billboards, transit displays, and public screens in malls, airports, and civic spaces—have become vulnerable targets for information warfare and psychological operations (PSYOPS). These networked displays function as "urban attention surfaces" that adversaries exploit by compromising content management systems and combining technical intrusion with AI-fabricated content including deepfakes, synthetic imagery, and voice cloning. This paper analyses real-world incidents demonstrating the threat: hackers displayed war propaganda on Kiev billboards (2014), hijacked a Cardiff screen for extremist imagery (2017), disabled Bristol Airport's flight displays via ransomware (2018), and attacked Taiwan's public screens during Pelosi's visit (2022). Case studies include the deepfake Zelenskyy surrender video, AI voice-clone robocalls impersonating a U.S. president, anti-war messages on Russian billboards, and AI-generated announcements on U.S. crosswalk systems. By tracing a consistent socio-technical attack chain across geopolitical contexts, this research provides security leaders, election authorities, and urban operators with a framework to harden DOOH ecosystems and measure resilience before these systems are weaponized at scale in fragile democracies.

Keywords: DOOH, deepfakes, PSYOPS, political manipulation, ransomware, public-address systems, socio-technical risk

¹⁵ IMPETUS, Skopje, North Macedonia

DIGITAL DIPLOMACY AND PUBLIC RELATIONS IN MENA: THE IMPACT OF SOCIAL MEDIA ON POLITICAL NARRATIVES AND SECURITY ASPECTS

Dusko Tomic¹⁶, Eldar Saljic¹⁷, Alwazna Falah¹⁸

Abstract: This study explores the transformative role of Artificial Intelligence (AI) in reshaping digital diplomacy, public relations, and security dynamics across the Middle East and North Africa (MENA) region. By integrating AI-driven analytics with social media monitoring, the research highlights how machine learning and algorithmic tools redefine the mechanisms of information dissemination, influence political narratives, and enhance cybersecurity frameworks. Findings reveal that AI-enabled technologies—such as automated content moderation, sentiment analysis, and predictive modelling—serve as double-edged instruments: while they empower governments and institutions to counter misinformation, manage crises, and engage global audiences, they also raise concerns about algorithmic bias, digital surveillance, and privacy violations. In the MENA context, AI facilitates both strategic narrative control and participatory engagement, reflecting the tension between innovation and restriction in authoritarian settings. The research underscores that over 68% of surveyed users expressed fear of surveillance, and over 70% practiced self-censorship, illustrating the pervasive impact of AI-enhanced monitoring on civic discourse. Ultimately, the study concludes that the future of digital diplomacy in MENA depends on adopting AI-driven yet ethically governed communication strategies—balancing security imperatives with transparency, inclusivity, and digital rights.

This work contributes to the emerging scholarship on AI in international communication, proposing a framework for responsible AI integration that safeguards user autonomy while reinforcing national and regional stability.

Keywords: Artificial Intelligence (AI); Digital Diplomacy; Social Media; Public Relations; MENA Region; Cybersecurity; Political Narratives; Algorithmic Governance; Disinformation; Surveillance; Self-Censorship; Digital Literacy; Data Ethics; National Security; Information Ecosystem

¹⁶ American University in the Emirates, UAE

¹⁷ American University in the Emirates, UAE

¹⁸ School of Engineering Management, “Union-Nikola Tesla” University, Belgrade, Serbia

RISK ASSESSMENT CONTENT CONCEPTUALIZATION FOR THE APPLICATION OF ARTIFICIAL INTELLIGENCE IN SECURITY SYSTEMS

Milica Mladenović¹⁹, Katarina Janković²⁰, Nenad Komazec²¹,

Abstract: The application of artificial intelligence in people's daily life has become inevitable, especially in the business environment. However, most organizations acknowledge the fact that the use of AI Systems is necessary, but guidelines are also necessary to adapt to the accelerated expansion of artificial intelligence. Security systems represent a particularly sensitive category when it comes to the application of artificial intelligence, given the huge unknowns about the risks that these systems carry with them. A substantive framework for risk assessment in this area is imposed as necessary because the existing risk assessment methods do not recognize AI risks, which makes their comprehensive assessment impossible. This paper provides a comprehensive conceptual content of the risk assessment of the application of AI in security systems, which includes risks during the entire life cycle of the AI system, which enables the identification, analysis, assessment and treatment of recognized risks and the monitoring and control of their impact on the system.

Keywords: risk assessment, artificial intelligence, AI, security system

¹⁹ Regional Association for Security and Crisis Management RABEK, Belgrade, Serbia,

²⁰ General Staff of the Serbian Army, Directorate for Development and Equipment J-5, Technical Test Centre, Centre for Testing Armaments and Military Equipment, Nikinci, Republic of Serbia,

²¹ University of Defence, Military Academy, Belgrade, Serbia,

ARTIFICIAL INTELLIGENCE AND SECURITY IN THE XXI CENTURY

PANEL II: ETHICAL AND LEGAL FRAMEWORKS

INTERCULTURAL ARTIFICIAL INTELLIGENCE: RECONCILING ETHICAL UNIVERSALISM AND CULTURAL DIVERSITY

Ernesta Molotkienė²²

Abstract: The paper explores how artificial intelligence (AI) can be developed to uphold universal moral values while remaining sensitive to cultural differences. As AI technologies increasingly shape human decisions across borders, questions arise about how ethical principles should guide autonomous systems in diverse societies. Ethical universalism promotes shared human values such as fairness, accountability, and respect for life, whereas cultural diversity emphasizes the moral norms and traditions unique to particular communities. This paper argues that reconciling these two perspectives is essential for creating globally trustworthy and locally legitimate AI. It introduces the concept of intercultural artificial intelligence, an approach that combines a universal ethical foundation with a culturally adaptive framework. This model prevents both ethical imperialisms, where one cultural view dominates, and moral relativism, which may undermine global cooperation. By integrating intercultural ethics, moral philosophy, and AI governance, the study outlines a pathway toward inclusive, context-aware, and human-centred AI. Such an intercultural approach enables the development of technologies that reflect both universal principles and cultural particularities, ensuring that artificial intelligence serves humanity as a whole.

Keywords: Intercultural Artificial Intelligence, Ethical Universalism, Cultural Diversity, AI Ethics, Moral Pluralism.

²² Klaipėda University, Klaipėda, Lithuania

**ARTIFICIAL INTELLIGENCE, A USEFUL ASSISTANT,
OR A PLAGIARISM THREAT: “ANALYSIS OF
REGULATORY APPROACHES AND ETHICAL
FRAMEWORK IN SERBIA AND IN THE EUROPEAN
UNION”**

Anila Jelesijevic²³

Abstract: The rapid integration of artificial intelligence (AI) into education system has challenged the line between the legitimate assistance and the academic plagiarism of the AI. This paper analyses how legislation and ethical frameworks in Serbia and the European Union (EU) regulate the role of AI in being a productive support tool and as a potential source of plagiarism. It also focuses on the theoretical debates of several scholars about the dual nature of AI with some of them highlighting the learning and creativity when AI used transparently and those who suggest few strategies but also instructions that academic staff can use to prevent plagiarism using AI. In addition to that, this paper has also taken into consideration surveys data of AI plagiarism in European universities and data of students' attitudes in Serbia when referring to the use of AI. This paper shows that while the use of AI into education system is increasing both in Europe and Serbia, in Europe despite for the comprehensive EU's AI regulatory laws, the practical enforcement and educational adaptation is still incomplete while in Serbia regulations are more at the stage of evolving strategy with advisory ethical guidelines. What is missing in both EU and Serbia's regulative is a clear distinguishing of when AI is a tool of plagiarism or not. The paper concludes that in defining the AI's role it is not sufficient not only to have the adequate legislation but also pedagogical and ethical development which besides enabling the capacities of the AI use also increase the awareness that AI is not a substitution of the human creativity.

Keywords: artificial intelligence, European Union, Serbia, legitimate assistance, plagiarism, regulatory laws

²³ Swiss Embassy, Belgrade, Serbia

Disclaimer: The opinions represented in this publication do not represent the official positions of the organizations in which its authors hold employment, nor do they represent the positions of the publishers of this Conference Proceedings, its editors, or its sponsoring organizations

DIGITAL JUS PACIS: LEGAL FOUNDATIONS FOR PEACE IN THE AGE OF ARTIFICIAL INTELLIGENCE

Troy Smith²⁴, Mikhail Byng²⁵

Abstract: This paper intends to explore artificial intelligence's (AI) transforming effect on global security and the existing gaps within legislative frameworks to manage the growing threats in this area, particularly the inability to manage "algorithmic warfare." The rapid advancement of AI technologies has outpaced international legal mechanisms, creating vulnerabilities in areas such as autonomous weapons systems, AI-enhanced cyber operations, and information warfare that existing treaties and conventions fail to adequately address. Introducing the idea of a digital jus pacis — a new legal-ethical framework for preserving peace in the AI era, the research will build on jus ad bellum and jus in bello but focus on preventing digital escalation, ensuring accountability, and protecting human dignity in cyberspace. Using case studies on autonomous defence, AI-driven intelligence, and cognitive warfare, it would propose three pillars for algorithmic peace, these include:

1. Lawful design (human oversight & proportionality)
2. Cooperative governance (regional & global alignment)
3. Moral restraint (digital humanitarian ethics)

The goal is to lay the groundwork for an AI Peace Compact and position digital jus pacis as a core principle of modern international law.

Keywords: Artificial Intelligence, Algorithmic Warfare, Digital Jus Pacis, International Security, AI Governance, Autonomous Weapons Systems, Cyber Operations, Human Oversight, Proportionality, AI Ethics, International Law, Jus ad Bellum, Jus in Bello, Cognitive Warfare, AI Peace Compact, Digital Humanitarian Law, Algorithmic Accountability, Cyber Escalation, Human Dignity

²⁴ Ministry of National Security, Trinidad and Tobago

²⁵ University of the West Indies, Trinidad and Tobago

APPLYING ENTERPRISE ARCHITECTURE FOR GOVERNANCE COMPLEXITIES IN TRANSNATIONAL UNIVERSITY ALLIANCES

Senne De Moor²⁶, Renata Petrevska Nechkoska²⁷

Abstract: The challenges in the lately present university alliances working towards European Degree are around the dual logic: a project-based mode driven by short-term milestones and deliverables, and an aspirational vision of becoming a long-term, mission-driven educational ecosystem. This creates friction between administrative coordination and strategic transformation. According to the CULT Committee’s evaluation of the European Universities Initiative (EUI), alliances often remain locked in a “project trap,” focusing on meeting contractual outputs rather than designing governance structures that endure beyond the funding. To move beyond this short-termism, university alliances require governance models that can support long-term institutional transformation while managing immediate operational demands. One promising approach lies in the application of enterprise architecture principles tailored to the higher education context. Transnational university alliances must navigate fragmented legal, administrative, and cultural landscapes while pursuing ambitious goals of interoperability, co-creation, and innovation. To support such institutional transformation, some authors propose a view-based Architecture Framework for Higher Education Systems (HES). This approach adapts enterprise architecture (EA) principles—particularly the TOGAF standard—to academic ecosystems and offers structured guidance for aligning governance, strategy, and communication across borders. Higher Education Systems function as complex socio-technical environments composed of diverse actors—students, faculty, administrative staff, policymakers—operating under different national contexts. Hence, a tailored Enterprise Architecture (EA) approach enables universities to manage this complexity by improving sense-making, systemic design, and collaborative alignment. Our research explores several European university alliances, such as: EU-CONEXUS, CHARM-EU, COLOURS, UNA Europa, CIVICA, 4EU+ and attempts to argue the rationale for Enterprise Architecture in Higher Education. By applying the Architecture Development

²⁶ Faculty of economics and business administration, Ghent University, Belgium

²⁷ Faculty of economics and business administration, Ghent University, Belgium and University St. Kliment Ohridski, Bitola, North Macedonia

Method (ADM) alliances can overcome strategic challenges like governance complexity and legal disparities, achieve more effective governance and interoperability. Our work is towards a reference architecture or “meta-model” that could guide alliance design across Europe. Such a model would support modular design of curricula, joint infrastructures, and strategic coordination across national boundaries. Our mapping of the interoperability flows across alliances enables discovery of learning opportunities in mobility, open programs, joint program scenarios. We also contribute with conceptual workflow of steps required to share and discover educational resources.

Keywords: Enterprise Architecture, European University Alliances, governance, discovery, interoperability

STRENGTHENING EU–MOROCCO COOPERATION ON ARTIFICIAL INTELLIGENCE AND CYBERSECURITY: A STRATEGIC IMPERATIVE FOR DIGITAL SECURITY AND SAHEL STABILIZATION

Yassine El Yattoui²⁸

Abstract: The intensification of geopolitical competition, the weaponization of information, and the rapid evolution of artificial intelligence (AI) technologies have transformed the digital sphere into a decisive domain of power, security, and influence. Within this context, cooperation between the European Union (EU) and the Kingdom of Morocco has emerged as a strategic axis for digital governance, cybersecurity, and information resilience in the Euro-Atlantic-African corridors. Scholars emphasize that cybersecurity has become inseparable from geopolitical influence and state sovereignty (Maleh & Maleh, 2022). Rooted in decades of political dialogue, security coordination, and intelligence exchange, the EU–Morocco partnership must now expand toward a more ambitious and structured framework centered on AI development, cyber-stability, and digital sovereignty. Such cooperation is no longer optional; it is a strategic necessity both for Europe’s southern security architecture and for Morocco’s role as a regional stability provider and technological bridge between Africa and Europe.

1. Historical Foundations and Strategic Rationale

For over two decades, EU–Morocco relations have been characterized by political stability, pragmatic cooperation, and shared strategic interests. Morocco was the first southern Mediterranean country to obtain an “Advanced Status” with the EU in 2008, reflecting its strategic importance as a reliable partner, a key economic hub, and a pillar of regional stability. Counter-terrorism coordination and intelligence exchange remain pillars of this privileged partnership, aligning with analyses that highlight Morocco’s central role in evolving security architectures in North Africa (Kezzoute, 2025). As cyber-threats grow and hybrid actors weaponize misinformation, Morocco and the EU share converging interests: safeguarding digital infrastructure, securing information flows, and preventing destabilizing narratives, particularly those emanating from the Sahel. Trust already exists, institutional bridges are solid, and shared security culture provides fertile ground for deeper digital cooperation, echoing arguments that contemporary alliances

²⁸ Lumière University Lyon II, Moroccan Centre for Research on Globalization (Morocco), Benemerita Universidad Autonoma de Puebla – BUAP (Mexico). Lyon, France

now hinge on technological and cyber collaboration (Kolade, 2024).

2. AI and Cybersecurity: A New Front in Euro-Moroccan Strategic Alignment

AI now structures geopolitical influence and national security capabilities. From intelligence analysis to infrastructure protection, emerging technologies expand the sophistication of state capacities. Cyber-sovereignty has become fundamental, with strategic infrastructures increasingly targeted by hostile actors (Maleh & Maleh, 2022). The EU's Artificial Intelligence Act and cybersecurity strategies demonstrate political ambition to shape global norms. Morocco has likewise embraced digital modernization, investing in AI ecosystems, cybersecurity infrastructures, and e-governance frameworks, consistent with academic assessments of its emerging digital-governance leadership (Kezzoute, 2025). A strengthened partnership would harmonize regulation, promote knowledge transfer, and build a shared digital security shield capable of addressing hybrid threats and securing innovation ecosystems across regions (Kolade, 2024).

3. The Sahel Imperative: Information Integrity and Security Governance

The Sahel remains one of the world's most volatile regions: a theatre of geopolitical rivalries, extremist sanctuaries, and disinformation warfare. The destabilization of Mali, Burkina Faso, and Niger, combined with international disengagement and hybrid foreign interventions, has intensified risks for Europe's southern border and Morocco's continental environment. Analysts show that European security structures in the Sahel face adaptation challenges in the face of shifting geopolitical vectors (Fortin, 2024). Extremist groups exploit digital platforms for recruitment and propaganda, while foreign actors weaponize information to erode Western partnerships. Morocco's counter-terrorism expertise and proximity to the Sahel reinforce its role as a stabilizing intelligence actor (McNair, 2024). Coordinated EU–Morocco digital cooperation can fortify monitoring mechanisms, cyber defence, and resilience capabilities across the region.

4. A Shared Normative Vision and the Challenge of Digital Sovereignty

Both the EU and Morocco defend a rules-based order rooted in transparency, sovereignty, and ethical governance. Strengthening AI and cybersecurity cooperation would reinforce this normative alignment, creating interoperable regulatory systems and countering authoritarian digital models. Morocco's diplomatic outreach and institutional reliability enable it to act as a continental anchor and a conduit between Africa and Europe, consistent with geopolitical

analyses positioning Africa and Europe as mutually indispensable partners in a shifting global order (McNair, 2024). Joint EU–Morocco technological frameworks can protect democratic values, secure digital infrastructures, and promote ethical AI development and deployment across borders (Kolade, 2024).

5. Recommendations and Future Directions

To turn shared vision into tangible capabilities, several strategic actions may be pursued:

- Establish an EU–Morocco Digital Security Council uniting cybersecurity agencies, intelligence networks, and academic/industrial partners.
- Create joint AI research hubs dedicated to predictive intelligence, cyber-resilience, and counter-disinformation.
- Develop integrated cyber training and certification programs for defence and intelligence officials focused on Sahel information ecosystems (Fortin, 2024).
- Harmonize regulation to create interoperable digital and AI governance frameworks aligned with European standards (Kezzoute, 2025).
- Launch a Euro-African Digital Security Initiative supporting cyber governance, infrastructure resilience, and counter-extremism in Sahelian states (McNair, 2024). Strengthened EU–Morocco cooperation is thus both mutually beneficial and strategically indispensable. Artificial intelligence and cybersecurity constitute the new frontiers of global power, and shared resilience demands structured partnership. Morocco and the EU have the opportunity, and responsibility, to pioneer an innovative trans-regional alliance capable of shaping the 21st-century security architecture and ensuring that the digital future rests on stability, sovereignty, and shared values (Maleh & Maleh, 2022; McNair, 2024).

Keywords: EU-Morocco Partnership, Digital Governance, Cybersecurity Cooperation, Artificial Intelligence, Cyber-Sovereignty, Information Resilience, Euro-Atlantic-African Corridors, Geopolitical Competition, Hybrid Threats, Digital Security

EU LEGAL REGULATIONS ON AI AND THEIR IMPACT ON THE SECURITY SECTOR

Javier Porras Belarra²⁹

Abstract: The regulation of artificial intelligence (AI) is emerging as a pivotal dimension of contemporary security policy, both domestically and internationally. The EU AI Act (adopted in 2024-25) represents the world's first comprehensive legal framework dedicated to AI systems within a major jurisdiction. Designing a risk-based regime that distinguishes between unacceptable, high and lower risk AI applications, the Act seeks to balance innovation and opportunity with safety, fundamental rights protection and accountability. We will explore how the EU AI Act is shaping the security sector (broadly defined to include cyber-security, law enforcement, intelligence, border management, critical infrastructure protection and defence support systems) and reflects on the legal and regulatory dimensions of AI's infusion into the security paradigm of the 21st century. First, the Act's tiered classification of risk (unacceptable, high, limited) creates a set of regulatory obligations that are especially salient for security actors. Under the "unacceptable risk" category, certain applications (for example social scoring based on behaviour, real-time remote biometric identification in public spaces) are prohibited in the EU, except under narrowly defined law-enforcement conditions. For those systems deemed "high risk" (including AI in critical infrastructure management, border control, law enforcement, migration and asylum systems), the Act mandates conformity assessments, registration in a dedicated EU database, lifecycle monitoring, and transparency. The second dimension therefore for the security domain is the introduction of traceability, human oversight, auditability, and incident-reporting obligations (features that reinforce accountability of AI use in security-relevant contexts). Second, from a national and international security perspective, the Act's implications extend beyond internal regulation. By establishing a harmonised EU-wide baseline, it affects how private-sector and public-sector AI suppliers structure their systems, how transnational supply chains operate, and how third-country actors engage with EU markets or collaborate via cross-border deployments. The regulation therefore shapes strategic technology flows, global standard-setting and geopolitical competition in AI and security. Third, the regulatory framework signals a shift in the security paradigm: AI is not only

²⁹ Public International Law Department, Spanish National University of Distance Education – UNED, Madrid, Spain

a tool for threat-actors (cyber-attacks, disinformation, autonomous weapon systems) but also a subject of governance. The EU AI Act reflects a normative effort to embed European values (safety, transparency, fundamental rights) into AI-enabled security operations. That raises new questions: How do security agencies adapt operationally in an environment of legal oversight and risk-based controls? To what degree does the Act's compliance architecture (testing environments, sandboxing initiatives for start-ups) support innovation in defence and security-oriented AI? Finally, this presentation will consider some of the key challenges and future directions: enforcement across heterogeneous member-states, the pace of AI advancement versus regulatory adaptation, balancing innovation with rights protection, and extending the notion of "security" to include resilience, cyber deterrence, and strategic competition in AI. In summary, the EU AI Act offers a pioneering regulatory template for the security sector (one that frames AI as both an enabler and regulated risk in the 21st century security architecture).

Keywords: EU AI Act, Legal Framework, Risk-Based Regulation, Regulatory Obligations, Conformity Assessment, Compliance Architecture, Harmonised EU-Wide Baseline, Regulatory Adaptation, Enforcement

ETHICAL DILEMMAS AND SOCIAL CHALLENGES WHO WILL TAKE THE RESPONSIBILITY FOR AI MISUSE?

Ida Manton³⁰

Abstract: The article will look into the phenomenon of artificial intelligence, the moral dilemmas rising from its widespread use and the necessity for regulating that use. As we are rushing towards creating the potentially most dangerous agent of automated decision-making we need to ask the question: whose responsibility is it to control the misuse of the AI and the potential damages it will inflict on our societies – the state, the tech corporations, or the individual. Information is the most valuable resource of our time. Information has always been precious, but the ways we access it have changed, and with that, so have the structures and methods by which it is shared. People have always been valued based on their knowledge, on how well they could use what they knew, and on how much creativity could stem from the information they gathered. The lead up to this new AI-driven reality has given us a preview of the difficulty with which our national and international bodies can regulate and legislate the use of unknown technologies. While we are still legislating services that were already set in motion by the tech giants in a legal vacuum, the AI became not only wide-spread but also a requirement in many areas of our everyday life, overnight. Without even having the time to process what this means, we are sending our AI produced content, AI enhanced CVs and AI proposed solutions as our own to AI supported platforms where our content and even overall existence is evaluated by AI on the other end. The text will therefore explore if the Artificial intelligence is intelligent, whether it is a tool that will be useful for humanity or will make people subservient to machines, and also what dangers are preventable and what is an integral part of the system, which we have to accept with making AI integral part of our lives. A part of the text will deal with the effects AI has on education, social dynamics that are already showing signs of pathologies which AI will only exacerbate, as well as the effect it will have on furthering polarization and creating echo-chambers that amplify dangerous group-think and changes in social and political interactions.

Keywords: AI, moral dilemmas, ethos, legislating, youth

³⁰ Consultant, trainer, lecturer and researcher in International Negotiations, New York, USA

USING ADVANCED TECHNOLOGIES IN ECOLOGICAL SECURITY CONCEPTS

Slobodan Simić³¹

Abstract: Accelerated development in the world is largely based on technical and technological innovations and achievements. Causal-consequential relationships are determined in many spheres of life, especially in segments essential for the survival of living beings. It is evident that the traditional approach to considering ecological security is largely outdated, that ecological dynamics due to environmental conditions have increased, and that it is necessary for ecological security segments and environmental constituents to begin to be viewed using advanced technologies. There are many reasons for these observations, established in a range from physical environmental protection to collecting, processing, analysing, and distributing large amounts of environmental information in an extremely short time. In this contextual plane, it becomes purposeful to use artificial intelligence in a wide range, from biodiversity protection to environmental monitoring in a compatible spectrum of activities. Software applications are becoming tools in the hands of scientific and professional workers in the field of ecological security. The multidimensional and multi-criteria analysis inherent in the genesis of artificial intelligence enables environmental monitoring in planning, organizational, and implementation activities, improves strategic decision-making and directing activities at global, regional, and local levels. Research in this field has a significant basis because the next period will bring challenges, risks, and threats that, in their intensity, data collection and processing needs, and action approach requirements, exceed the ability of humans, as sentient beings, to timely comprehend differential impacts on people, animals, and plants. These constructs are further substantiated by the fact that artificial intelligence will help process impacts on living beings from space. The aim of this work is the imperative use of artificial intelligence in the field of ecological security in accordance with the vulnerability of life cycles complicated by global changes in the natural environment.

Keywords: Artificial Intelligence, Ecological Security.

³¹ Security Research Centre, Banja Luka, Bosna i Hercegovina

ARTIFICIAL INTELLIGENCE AND SECURITY IN THE XXI CENTURY

PANEL III: THE AI ERA BENEFITS AND THREATS

AI-BASED PREDICTIVE MODELING OF STUDENT PERFORMANCE IN MOODLE INFRASTRUCTURES: A CASE STUDY FROM THE EUROPEAN UNIVERSITY ALLIANCE COLOURS

Andrijana Bocevska³², Renata Petrevska Nechkoska³³, Vasko Sivakov³⁴,

Abstract: European university alliances aim to enhance student performance and enable personalized learning through the integration of digital platforms and intelligent tools that support teaching and learning processes. This paper explores the application of Artificial Intelligence (AI) to predict students at risk of academic failure by analyzing their activity within Moodle, a widely used e-learning platform. Our case study is the European university alliance COLOURS and its Moodle platforms across each partner university, but also the interoperable infrastructures set on Alliance level (be it Moodle of Moodles or specially designated aggregators and portals). The analysis considers multiple indicators, including the number of completed assignments, hours spent studying, participation in discussion forums, attendance in learning activities, and engagement with digital resources such as learning materials, quizzes, and simulations. We intend to incorporate quantitative data first, but at later stages of the research, also qualitative aspects, as well as diverse contexts. For the purposes of the COLOURS alliance analysis, a Random Forest machine learning model is implemented in Python using Google Colab to analyze Moodle activity data and predict at-risk students. Student activity data are collected from Moodle through a Learning Record Store (LRS), which ensures standardized xAPI statements and reliable data extraction. This approach leverages the rich dataset collected in Moodle and the predictive capabilities of AI to support early risk detection and personalized learning recommendations. The expected outcome is the early identification of at-risk students, enabling timely interventions and contributing to the development of more effective, personalized learning strategies that enhance academic achievement.

Keywords: Artificial Intelligence, COLOURS Alliance, Random Forest, At-Risk Students, Predictive Modelling, Learning Analytics, Interoperability, Moodle

³² Faculty of Information and Communication Technology, University St. Kliment Ohridski, Bitola, North Macedonia,

³³ Faculty of Economics, University St. Kliment Ohridski, Bitola, North Macedonia and Ghent University Belgium

³⁴ Head of IT Department, Rectorate of University St. Kliment Ohridski, Bitola, North Macedonia

VISION TRANSFORMERS FOR FINGERPRINT EMBEDDING GENERATION: EVALUATION ON CASIA DATASET

Milos Zivadinovic³⁵, Bojan Jovanovic³⁶

Abstract: This paper investigates the application of Vision Transformers (ViTs) for generating discriminative fingerprint embeddings. We employ the standard ViT architecture with 16×16 patch size, originally designed for natural image classification, and adapt it for fingerprint biometric encoding using triplet loss optimization. Our approach treats fingerprint images as sequences of patches, leveraging the self-attention mechanism of transformers to capture both local ridge patterns and global fingerprint structure. We evaluate our method on the CASIA Fingerprint Database, conducting verification experiments with 114 genuine pairs and 114 impostor pairs. The results demonstrate strong performance, achieving a ROC AUC of 0.9899 and an Equal Error Rate (EER) of 4.82%. These results indicate that Vision Transformers, without fingerprint-specific architectural modifications, can effectively learn discriminative embeddings for fingerprint recognition. The success of this approach suggests that transformer-based architectures represent a viable alternative to conventional methods, opening new directions for biometric feature extraction using attention mechanisms.

Keywords: Vision Transformers (ViT), Fingerprint recognition Biometric authentication, Triplet loss, Fingerprint embeddings

³⁵ Faculty of Organisational Sciences, University of Belgrade, Serbia,

³⁶ Faculty of Organisational Sciences, University of Belgrade, Serbia,

UNDERSTANDING CONSUMER TRUST IN AL – ENABLED MARKETING: A QUALITATIVE ANALYSIS OF EMOTIONAL REACTIONS TO CHATBOTS

Esma Nur Cerinan Otovic³⁷, Murat Aytas³⁸, Ivana Savic³⁹

Abstract: Artificial intelligence is an active part of marketing world and applications, especially for integrating and communicating with customers. Artificial intelligence, which contributes to the personalization marketing strategy emphasized by today's marketing world and accelerates communication, also appears as a problem that affects consumer trust and loyalty and general acceptance. This study examines people's emotional approaches and reactions to artificial intelligence- supported chat, while also examining how the communication process with Chatbot affects trust formation. Three distinct emotions emerged within this theme. While the rapid response and detection of AI-powered Chat boxes increased the satisfaction and trust, Chat boxes' overly automated responses and lack of emotion, combined with their monotonous approach, created feelings of frustration and anxiety. Furthermore, database security concerns about protecting personal information were also raised. One common point participants mentioned was the trust and satisfaction that Chat boxes' ability to solve tasks without human intervention gave them. However, their limited-service provision, where empathy was required, undermined trust and created concerns. This raises the dilemma of whether chat boxes are good marketing communication tool or a trust problem, this study highlights the importance of trust, individuality, and empathy in developing customer relationships through the communication process established by AI powered marketing tools. While it is suggested that the negative impacts of AI- powered communication tools can be mitigated by incorporating more human-like features, such as a more natural language and adjustments, it also discusses the precise role of these applications in communication within the marketing world.

Keywords: Artificial intelligence, Chatbot, Marketing

³⁷ Faculty of Management Herceg Novi, University Adriatic Bar, Montenegro

³⁸ Faculty of Communication, Selcuk University, Turkey

³⁹ Faculty of Management Herceg Novi, University Adriatic Bar

AI DEEPPFAKE TECHNOLOGY

Ana Kosanović⁴⁰, Borjana Georgiou Sekuloski⁴¹, Ratko Stajić⁴², Lazar Bezbradica⁴³

Abstract: The development of artificial intelligence has led to major technological advancements but has simultaneously created new ethical and security challenges, most notably the emergence of deepfake technology stands out. Based on neural networks, this technology enables the creation of highly realistic yet fabricated audio-visual content, threatening information integrity and public trust. This paper presents a systematic analysis of recent scientific and professional literature, focusing on deepfake technologies and their ethical implications. Sources include databases such as PubMed, Google Scholar, IEEE Xplore, and leading journals in information technology and ethics. Researches from 2025. indicate a drastic rise in both the volume and sophistication of deepfake content, posing growing risks to online security. Deepfake files are projected to reach 8 million by the end of 2025, compared to half a million in 2023. Furthermore, human detection accuracy for high-quality deepfakes remains low, averaging only 24.5%. This study aims to examine models, algorithms, and strategies for their identification and mitigation.

Keywords: artificial intelligence, disinformation, deepfake, ethics.

⁴⁰ School of Engineering Management, “Union-Nikola Tesla” University, Belgrade, Serbia

⁴¹ School of Engineering Management, “Union-Nikola Tesla” University, Belgrade, Serbia

⁴² School of Engineering Management, “Union-Nikola Tesla” University, Belgrade, Serbia

⁴³ School of Engineering Management, “Union-Nikola Tesla” University, Belgrade, Serbia

AI-DRIVEN PHISHING ATTACKS: EMERGING THREATS AND SECURITY STRATEGIES

Toni Nakovski⁴⁴, Natasha Blazheska-Tabakovska⁴⁵, Mimoza Bogdanoska Jovanovska⁴⁶

Abstract: The rise of generative AI has led to a new era of sophisticated phishing attacks. The proposed paper, "AI Phishing Attacks", explores this evolving threat, where malicious actors use AI to create personalised, convincing phishing campaigns at scale. We analyse attack techniques, from automated content generation to deepfakes, and assess their impact. The paper argues that traditional defences are insufficient, necessitating a multi-layered approach combining AI-powered security solutions with robust user awareness programs. We also examine the ethical and social implications of malicious AI, advocating for a collaborative approach to develop effective countermeasures and regulatory frameworks. This paper provides valuable insights for the cybersecurity community and outlines a forward-looking strategy to counter the escalating threat of AI-augmented phishing, emphasising the urgent need to redefine security paradigms for the 21st century.

Keywords: Artificial Intelligence, AI-augmented phishing, Attack Techniques, AI-powered security solutions

⁴⁴ Faculty of Information and Communication Technologies - Bitola, University "St. Kliment Ohridski", Bitola, Republic of North Macedonia

⁴⁵ Faculty of Information and Communication Technologies - Bitola, University "St. Kliment Ohridski", Bitola, Republic of North Macedonia

⁴⁶ Faculty of Information and Communication Technologies - Bitola, University "St. Kliment Ohridski", Bitola, Republic of North Macedonia

ARTIFICIAL INTELLIGENCE (AI) IN EDUCATION AND RESEARCH

Vera Arezina⁴⁷

Abstract: After brief history of Artificial intelligence (AI), we will point out the EU definition of an AI as a machine-based system designed to operate with varying levels of autonomy which can generate outputs such as predictions, recommendations or decisions in many fields, as well in education and research. Upon different criteria, we differ AI as an (a) object or (b) subject. As object, we can differ AI to narrow and generative AI. Narrow AI is program or system designed for a set task, such as language translation, to mark basic content, data analysis, sorting images, or list of literature. Generative AI can create new content by learning patterns from existing data, such as *ChatGPT* and *Claude* for content generation and writing essays and papers or *Perplexity* for fact-checking and research and others. AI as (b) subject may differ to super AI, which can understand and model human emotions, context or intentions, and Self-aware AI. Regarding AI as a subject, many issues are still debated such as necessity, consciousness and accountability or control upon AI. In this paper we will point out advantages and risks of applying AI in education and research. Artificial intelligence may become a key driver of change in education. It can significantly improve the quality and accessibility of education as well to improve data analysis in research, but at the same time questions arise about ethics, intellectual property protection and other possible negative consequences.

Key words: artificial intelligence (AI), education, research, data analysis

⁴⁷ Faculty of Political Sciences, University of Belgrade, Belgrade, Serbia

ARTIFICIAL INTELLIGENCE IN MEDICAL DIAGNOSTICS: A CRITICAL NARRATIVE REVIEW OF RISKS, RESPONSIBILITY, AND THE EPISTEMOLOGICAL LIMITS OF LARGE LANGUAGE MODELS

Marjan Marjanović⁴⁸, Luka Latinović⁴⁹

Abstract: The rapid integration of artificial intelligence (AI) into diagnostic medicine represents both a technological advance and an epistemological disruption. This narrative critical review examines how large language models and related AI systems influence diagnostic reasoning, clinical accountability, and medical ethics. While AI has demonstrated remarkable potential in pattern recognition and data synthesis, its correlation-based logic lacks causal understanding, interpretability, and moral agency. The review identifies key risk domains including automation bias, dataset bias, model opacity, and liability asymmetries between developers and physicians. It argues that AI's integration challenges traditional boundaries of professional responsibility and informed consent, raising concerns over epistemic validity and patient trust. Current governance frameworks, adapted from static medical device regulation, remain ill-suited for continuously learning systems. The research shows that safeguarding the integrity of medical reasoning in the age of AI requires a renewed commitment to epistemic humility, distributed accountability, and the preservation of human judgment within computationally mediated care.

Keywords: epistemic integrity; diagnostic reasoning; medical accountability; automation bias; regulatory ethics.

⁴⁸ Clinic for General, Visceral and Thoracic Surgery - InnKlinikum, Altötting, Germany

⁴⁹ School of Engineering Management, "Union - Nikola Tesla" University, Belgrade, Serbia

**RELIABILITY AND SECURITY OF AI MODELS IN
HARDWARE SYSTEMS: THE ROLE OF EXPERT
KNOWLEDGE AND TECHNICAL TALENT
MANAGEMENT**

Ivana Bojić⁵⁰

Abstract: This paper discusses how the management of technical talent and knowledge sharing contribute to the reliability of AI-based hardware systems. It explores practical means of supporting engineers through continuous learning, collaboration between teams, and maintenance of key experts within the organization. Special attention is given to the role of AI tools in verification work, which simultaneously brings about new risks associated, above all, with data protection and ethical use. The quality of AI systems thus depends not only on algorithms and hardware but also, and most importantly, on how technical teams are guided, developed, and connected.

Keywords: AI models, hardware systems, technical talent management

⁵⁰ School of Engineering Management, “Union - Nikola Tesla” University, Belgrade, Serbia

THE SECURITY RISKS OF AI CHAT SYSTEMS IN SENSITIVE HUMAN DOMAINS

Olga Mašić⁵¹, Ana Jurčić⁵², Dejan Živković⁵³

Abstract: The rapid advancement of conversational artificial intelligence (AI) has transformed how individuals seek information, guidance, and emotional support. While AI chat systems offer accessibility, immediacy, and personalization, their unregulated use in high-stakes contexts, such as mental health counselling, medical advice, and financial decision-making, presents significant ethical, security, and safety risks. This paper investigates the dangers of AI-assisted advice where misinterpretation, contextual misunderstanding, or algorithmic bias can lead to harmful outcomes. Employing a qualitative multiple case study methodology, the research analyses publicly documented incidents of AI-driven misinformation and unsafe guidance, supported by content analysis, policy review, and expert interviews in AI ethics, cybersecurity, and clinical psychology. The study explores how the probabilistic reasoning and synthetic empathy of large language models create a false perception of understanding, potentially amplifying risk in emotionally charged or high-stakes interactions. Findings reveal systemic vulnerabilities in model architecture, inadequate harm-prevention mechanisms, and insufficient governance standards. The paper concludes by proposing a risk governance framework that integrates algorithmic transparency, human-in-the-loop oversight, and adaptive threat detection to mitigate user harm. The results highlight the urgent need for interdisciplinary collaboration between technologists, regulators, and mental health professionals to ensure that conversational AI remains a secure and responsible tool of assistance rather than inadvertent harm.

Keywords: conversational artificial intelligence, AI ethics, cybersecurity

⁵¹ School of Engineering Management, “Union - Nikola Tesla” University, Belgrade, Serbia

⁵² School of Engineering Management, “Union - Nikola Tesla” University, Belgrade, Serbia

⁵³ School of Engineering Management, “Union - Nikola Tesla” University, Belgrade, Serbia

EMPLOYEE-DRIVEN LEAKAGE OF TECHNICAL DOCUMENTATION INTO GENERAL-PURPOSE LLMs — A CRITICAL NARRATIVE REVIEW

Luka Latinović⁵⁴, Oleg Zhukovskiy⁵⁵, Olga Mašić⁵⁶, Dejan Živković⁵⁷

Abstract: Employees increasingly consult general-purpose large language models (LLMs) for routine engineering tasks, and model suggestions flow into technical documentation. In parallel, employees may paste or upload excerpts from proprietary artefacts. This bidirectional exchange plausibly exposes documentation to external systems and allows model-mediated knowledge to diffuse across organisations. This critical narrative review maps leakage mechanisms within the documentation lifecycle and proposes proportionate controls and evaluation practices. Evidence is heterogeneous, and provider policies shift frequently globally; provider statements are treated as time-stamped observations, and prevalence is not asserted. Findings indicate that risk concentrates at transition points—copy–paste, upload, connector invocation, and paste-back—amplified by intermediaries, operational logging, weak classification, and incentives that reward speed. We present a typology of pathways and a minimal guardrail stack that are contractable and auditable. The evaluation framework comprises qualitative risk scoring, rule-based escalation, and simple metrics: coverage of sanctioned egress, adoption ratio, blocking effectiveness, false-positive rate, drift lag, and mean time to a compliant alternative. Limitations include under-reporting, attribution uncertainties, and sectoral bias. The review aims to support cautious adoption by making assumptions explicit and privileging mechanism-centred governance.

Keywords: data exposure, data exfiltration, training capture, shadow IT, AI governance, model-mediated knowledge transfer, egress.

⁵⁴ School of Engineering Management, “Union - Nikola Tesla” University, Belgrade, Serbia

⁵⁵ MART-INFO LLC (ООО «МАРТ-ИНФО»), Moscow, Russian Federation

⁵⁶ School of Engineering Management, “Union - Nikola Tesla” University, Belgrade, Serbia

⁵⁷ School of Engineering Management, “Union - Nikola Tesla” University, Belgrade, Serbia

APPLICATION OF MACHINE LEARNING IN INDUSTRIAL SAFETY: DIGITAL INNOVATIONS AND NEW SAFETY PARADIGMS IN REFINERY PROCESSES

Luka Abramović⁵⁸, Jelena Raut⁵⁹

Abstract: In modern refinery facilities, complex industrial processes require a high level of safety to minimize risks to human lives, property, and the environment. Traditional monitoring systems and safety procedures increasingly show limitations in detecting anomalies and predicting potential incidents. The application of machine learning (ML) in industrial safety enables a transformation of safety paradigms through the analysis of large volumes of data from sensors, SCADA systems, and other industrial sources. This paper explores current digital innovations in ML algorithms for predictive analytics, automatic anomaly detection, and optimization of safety procedures in refinery processes. Focus is placed on integrating ML models into existing risk management systems, implementation challenges, and opportunities for enhancing industrial safety through a proactive approach. The research results indicate that the application of machine learning significantly contributes to reducing incidents, improving the efficiency of safety operations, and opening new perspectives for digital transformation in industrial safety.

Keywords: machine learning, industrial safety, refinery processes, digital innovations, predictive analytics

⁵⁸ Total Energies Refinery, Antwerpen, Belgium

⁵⁹ School of Engineering Management, “Union - Nikola Tesla” University, Belgrade, Serbia

THE ROLE OF HIGHER EDUCATION IN DEVELOPING ETHICAL AND SECURITY AWARENESS FOR THE RESPONSIBLE USE OF ARTIFICIAL INTELLIGENCE

Nataša Sunarić⁶⁰, Brankica Pažun⁶¹, Milena Cvjetković⁶²

Abstract: The rapid development of artificial intelligence (AI) has led to significant changes in work processes and structures, educational practices, and social relations within a short period of time. The very application of AI enhances efficiency, innovation, and access to information; however, it also raises serious concerns about ethics, security, and data privacy protection. The aim of this paper is to analyze the role of higher education in shaping ethical and security awareness within academic processes that use artificial intelligence as a tool. The primary task of the academic community is to ensure the responsible, secure, and transparent use of artificial intelligence in everyday practice through curricula design and pedagogical approaches. Joint efforts of the research sector, international organizations, and academic networks towards establishing new standards should focus on creating frameworks that enable the development of academic professionals capable of using AI tools safely and in accordance with ethically acceptable codes of conduct. Survey results show that most universities in Western Europe have already established programs addressing ethical and security aspects of AI technologies, while universities in Southeastern Europe are still in the process of developing institutional policies in this regard. Therefore, this paper proposes a model for integrating AI ethics and security into educational processes in higher education of Southern European countries, as well as the establishment of ethics committees at the institutional level, which would contribute to the responsible use of artificial intelligence in higher education institutions in the future.

Keywords: artificial intelligence, ethics, higher education, digital literacy.

⁶⁰ School of Engineering Management, “Union - Nikola Tesla” University, Belgrade, Serbia

⁶¹ School of Engineering Management, “Union - Nikola Tesla” University, Belgrade, Serbia

⁶² School of Engineering Management, “Union - Nikola Tesla” University, Belgrade, Serbia

DIGITAL INNOVATIONS IN INTELLIGENCE DECISION-MAKING SYSTEMS: THE ROLE OF MACHINE LEARNING

Jelena Raut⁶³, Darko Mačkić⁶⁴

Abstract: Modern intelligence systems are undergoing a profound transformation driven by digital innovations, with machine learning (ML) emerging as a key tool for enhancing decision-making processes. The rapid development of information technologies enables a shift from traditional, manual analysis methods to automated and predictive models, allowing faster processing of large volumes of heterogeneous data from various sources, including IoT sensors, satellite imagery, network traffic, and social media. This paper provides a systematic review of the theoretical foundations and practical applications of ML in intelligence systems, analysing supervised, unsupervised, and deep learning, their advantages and limitations, as well as their impact on decision-making accuracy and efficiency. Special attention is given to the challenges of ML implementation, including technical aspects (data heterogeneity and high dimensionality), security risks (model attacks, data leaks), and ethical dilemmas (algorithmic bias, transparency, and user trust). The literature and empirical studies indicate a growing trend of integrating ML with multi-criteria decision-making (MCDM) methods, human-in-the-loop models, and explainable AI (XAI), enhancing risk control and decision interpretability. Future development directions include increasing model robustness, adaptability to new threats, and synergy with other digital technologies such as blockchain and quantum analytics. The study concludes that machine learning is a tool for improving the efficiency, accuracy, and resilience of intelligence systems, while human oversight remains essential for sustainable application in a dynamic digital environment.

Keywords: digital innovations, intelligence systems, machine learning, automation, XAI

⁶³ School of Engineering Management, "Union - Nikola Tesla" University, Belgrade, Serbia

⁶⁴ Metal doo, Obrenovac, Serbia

ENHANCING AIRPORT SECURITY SYSTEMS: INTEGRATING ARTIFICIAL INTELLIGENCE FOR THREAT DETECTION AND PASSENGER FLOW OPTIMIZATION

Hamad Hassan Ahmad⁶⁵

Abstract: This paper explores the integration of artificial intelligence (AI) into airport security systems to enhance threat detection and optimize passenger flow. Adopting a traditional academic framework, the study begins with an introduction, followed by an extensive review of literature addressing key subtopics: the general applications of AI, its specific role in security, an overarching analysis of airport security systems, strategies for passenger flow optimization, and the implementation of AI for threat detection and flow management. Subsequent chapters delve into the application of AI to the unique challenges faced by airports in the United Arab Emirates (UAE). Employing both SWOT analysis and TOWS matrix methodologies, the study identifies strategic opportunities and constraints inherent to integrating AI-driven solutions. Alternative strategies are presented, addressing the practical implementation of AI in UAE airports with an emphasis on enhancing security efficacy and operational efficiency. The final sections discuss the findings, synthesizing insights from the literature review, SWOT analysis, and TOWS matrix. Three critical strategies are emphasized as foundational for optimizing airport security systems and passenger experiences in UAE airports. This research aims to contribute to the advancement of AI technologies in aviation security, offering vital solutions for contemporary challenges and setting a benchmark for innovation in global airport management.

Keywords: Artificial intelligence, airport security, threat detection, passenger flow, United Arab Emirates.

⁶⁵ American University in the Emirates, UAE

LLMS IN HIGHER EDUCATION (2025): OVERVIEW OF ISSUES, ETHICS, INTEGRITY AND INSTITUTIONAL POLICY

Michal Hanák⁶⁶, Jozef Zaíko⁶⁷

Abstract: Large Language Models (LLMs) have become a common feature of the higher education environment between 2022 and 2025: as personal “tutors”, feedback generators, assignment design tools and administrative assistants. At the same time, systemic issues of integrity, assessment, privacy and fairness are emerging. This review summarizes the state of knowledge and policies in 2025 with an emphasis on the university context, draws on academic studies, international guidelines and institutional practice, and suggests realistic “guardrails” for responsible deployment. (UNESCO, 2023; US Department of Education, 2023; QAA, 2023).

Keywords: Large Language Models, higher education, design tools

⁶⁶ Faculty of Civil Engineering, Brno, Czech Republic

⁶⁷ The European Institute of Additional Education, Pothajska, Slovak Republic

THE ROLE OF INNOVATIVE TECHNOLOGIES IN CRITICAL INFRASTRUCTURE PROTECTION WITH A SPECIAL FOCUS ON DUBAI AIRPORT

Amir Abdalla Hassan Al Ali⁶⁸

Abstract: This paper investigates the role of innovative technologies in critical infrastructure protection, with a special focus on Dubai International Airport as a global leader in aviation security innovation. Drawing upon a comprehensive literature review, a structured brainstorming session with stakeholders, and strategic analyses (SWOT and TOWS), the study explores how advanced systems such as artificial intelligence, biometric identification, Internet of Things (IoT) sensors, and predictive analytics can be integrated to address contemporary security challenges. Airports are identified as uniquely complex nodes within national and international transport networks, requiring both physical and cyber protection measures. The findings reveal that Dubai International Airport's strengths lie in substantial technological investment, strong governmental support, and an innovation-driven strategic culture. However, challenges persist in areas such as cybersecurity vulnerabilities, rapid technological obsolescence, and the need for continuous workforce training. The strategic framework developed in this thesis recommends leveraging technological leadership to expand global collaboration, enhance system interoperability, and strengthen cyber resilience. Ultimately, the research concludes that the effective protection of critical infrastructure depends on a balanced integration of cutting-edge technology, institutional readiness, and adaptive policy frameworks, positioning Dubai Airport as a benchmark for global best practices in security innovation.

Keywords: critical infrastructure protection; innovative technologies; airport security; Dubai International Airport; artificial intelligence; biometrics; IoT; cybersecurity; SWOT analysis; TOWS matrix; strategic security management

⁶⁸ American University in the Emirates, UAE

Security Aspects of Smart Cities - Case Study Dubai

Eisa Ahmed Abdalla Hussain Al Hammadi⁶⁹

Abstract: The cities of today are undergoing innovative transformation. Transformations of cities to smart cities, not only changes the approach to their function, but also changes the lives of the smart city inhabitants. Smart cities are transformed by the use of information technologies and include various segments like smart governing, smart economy, smart environment, smart transportation, smart energy, smart healthcare, smart education, smart people (smart human resources). However, one of the most important topics of smart cities that interconnects all other topics is the security of smart cities. As smart city security is a vital feature of smart city operations, it is very important to analyse this issue. This thesis is concentrating on the scientific analysis of the smart city phenomenon with the focus on the issue of the smart cities' security. The thesis specifically analysed all aspects of smart cities, security of smart cities and the example of smart city and smart city security concept on the example of Dubai as one of the most advanced smart city in the world. The methods used were qualitative analysis of the literature, the case study, and the experts' discussion group, with application of SWOT analysis for development of recommendations for future analyses and implementations of smart city concept. Major findings included the application of appropriate security strategies, emphasis on innovative aspect of information technologies, education of citizens on the benefits of smart cities and development of risk management strategies. It can be concluded that as smart city security is a key aspect of smart city functioning as all elements of smart city must keep in mind the concept of security and ensure the safe functioning of all initiatives and principles.

Keywords: smart cities, security, information technologies, Dubai.

⁶⁹ American University in the Emirates, UAE

Ethics and Responsibility in Artificial Intelligence Use: A Literature Review

Dragana Nikolić-Ristić⁷⁰, Violeta Jovanović⁷¹,

Abstract: The rapid and continuous development of artificial intelligence (AI) and its integration across almost all fields brings greater efficiency and opportunities for economic, social, and technological improvements. At the same time, complex ethical issues and responsibility for AI use arise. This paper examines various aspects of AI utilization, including ethical and social challenges. The aim of the study is to provide a systematic literature review on ethical considerations and responsibility in the use of AI technologies. The literature review was conducted using the PRISMA methodology, covering scientific articles published between 2020 and 2025. The paper emphasizes the importance of integrating ethical principles into the AI usage process to minimize risks and maximize benefits. Ethics and responsibility in AI use should remain a focus of future research as technology continues to develop.

Keywords: Ethics, Responsibility, AI

⁷⁰ Faculty of Management, Metropolitan University Belgrade

⁷¹ Faculty of Management, Metropolitan University Belgrade

УЛОГА ВЕШТАЧКЕ ИНТЕЛИГЕНЦИЈЕ У НЕУТРАЛНОСТИ РЕПУБЛИКЕ СРБИЈЕ: ИЗАЗОВИ И ПЕРСПЕКТИВЕ

Александар М. Павић⁷², Хатица А. Бериша⁷³

Апстракт: Политика војне неутралности представља један од темељних принципа савремене спољне и безбедносне политике Републике Србије. У епохи вештачке интелигенције, овај концепт добија нову димензију, технолошку неутралност као услов стратешке аутономије. Развој и примена вештачке интелигенције не само да утичу на војне способности, већ обликују односе моћи, економску зависност и когнитивну контролу унутар глобалног система. У таквом контексту, питање неутралности више се не односи искључиво на војно савезништво, већ на способност државе да управља сопственим дигиталним суверенитетом и одржи равнотежу између различитих технолошких сфера утицаја. Војно савезништво се може и треба разматрати у контексту неутралности, али не као чланство, већ као референтни оквир стратешке оријентације и ограничења. Рад полази од претпоставке да вештачка интелигенција постаје кључни фактор у дефинисању нових облика стратешке зависности и отпорности. Србија, позиционирана између западних и источних технолошких система, суочава се са изазовом да своју неутралност прошири у домен алгоритамске политике и дигиталне инфраструктуре. Уместо блоковског сврставања, вештачка интелигенција може постати инструмент интелигентног балансирања, средство којим држава јача сопствене аналитичке, комуникационе и безбедносне капацитете, задржавајући контролу над подацима и процесима од националног значаја. Закључно, у раду се предлаже концепт „интелигентне неутралности“, који подразумева интеграцију принципа дигиталног суверенитета, етичке одговорности и технолошке независности у оквир стратешке културе Србије. Тај модел може послужити као теоријска и практична основа за развој новог типа неутралности у дигиталној ери, неутралности која не почива на изолацији, већ на активној контроли алгоритамских токова моћи. Србија тиме добија прилику да постане пример адаптивне државе која не само одолева утицајима великих

⁷² Војна Академија, Универзитет одбране у Београду, Србија

⁷³ Школа националне одбране „ Војвода Радомир Путник “, Универзитет Одбране у Београду, Србија

сила, већ обликује сопствени дигитални идентитет унутар мултиполарног поретка.

Кључне речи: интелигентна неутралност, адаптивна држава, вештачка интелигенција, технолошка неутралност.

SECURITY AND PROTECTION OF CRITICAL INFRASTRUCTURE IN BIH- LEGAL FRAMEWORK

Radislav Jovičić⁷⁴, Dražan Erkić⁷⁵

Abstract: In an era of escalating global instability characterized by complex geopolitical tensions, technological disruptions, and emerging security challenges, the protection of critical infrastructure has become paramount. Bosnia and Herzegovina (BiH), as a constitutionally complex state, faces unique challenges in developing robust security frameworks. This paper explores the intersection of artificial intelligence (AI) technologies and critical infrastructure security, examining how advanced computational methods can enhance legislative and strategic approaches to national protection. The research investigates the potential of AI-driven risk assessment and predictive modelling in identifying and mitigating potential threats to critical infrastructure. By leveraging machine learning algorithms and data analytics, the study proposes innovative strategies for strengthening security systems across local, national, and international domains. The analysis delves into the multifaceted nature of security challenges, drawing insights from recent global events such as terrorist incidents, financial crises, pandemics, and regional conflicts. Furthermore, the paper critically examines the existing legislative framework in BiH, highlighting the intricate layers of governmental responsibilities. Through a comprehensive analysis, it demonstrates how AI technologies can support more adaptive, intelligent, and proactive security mechanisms. The research ultimately aims to provide actionable recommendations for integrating advanced technological solutions into the national security infrastructure, addressing the complex security landscape of contemporary geopolitical environments.

Keywords: security, critical infrastructure, artificial intelligence, legislative framework, risk assessment, national protection

⁷⁴ High School for Service Business East Sarajevo - Sokolac, Bosnia and Herzegovina

⁷⁵ Faculty of Security Sciences; University of Banja Luka, Bosnia and Herzegovina

AI AS A STRATEGIC SECURITY TOOL IN GOVERNMENT DECISION MAKING

Ibrahim Ali Alhudaïdi⁷⁶, Stanko Bulajić⁷⁷

Abstract: Artificial intelligence is increasingly embedded in the strategic decision-making architecture of modern governments, offering unparalleled analytical capability, scenario modelling, and early-warning functions across security-critical domains. This article critically examines AI's role as a strategic security tool in government decision making, arguing that its value lies not merely in automating analysis but in reshaping the speed, scope, and epistemic basis of state-level security judgments. The study integrates contemporary literature, policy documents, and empirical cases to explore three key dimensions: (1) AI-enabled situational awareness and predictive intelligence, including real-time threat detection and strategic foresight; (2) decision augmentation, whereby machine-learning systems influence tactical and long-range governmental choices, often under uncertainty; and (3) governance and risk constraints, including information asymmetry, algorithmic opacity, adversarial manipulation, and ethical-legal accountability. Findings indicate that AI enhances state resilience by reducing cognitive load, improving probabilistic assessment, and enabling continuous risk monitoring. However, structural vulnerabilities persist, particularly related to model bias, cyber-exposure, and a widening capability gap between technologically advanced and resource-constrained governments. The article concludes that effective deployment of AI in strategic security contexts requires robust oversight frameworks, interdisciplinary evaluation mechanisms, and the integration of explainable, provenance-aware AI systems to preserve democratic legitimacy while maintaining decision superiority.

Keywords: epistemic integrity; diagnostic reasoning; medical accountability; automation bias; regulatory ethics.

⁷⁶ Ministry of Foreign Affairs, United Arab Emirates

⁷⁷ School of Engineering Management, "Union - Nikola Tesla" University, Belgrade, Serbia

BEYOND THE BATTLEFIELD: THE ETHICAL IMPLICATIONS AND REGULATORY CHALLENGES OF USING AUTONOMOUS AI SYSTEMS FOR ENVIRONMENTAL SECURITY AND RESOURCE PROTECTION?

Aleksandar Ivanov⁷⁸, Kire Babanoski⁷⁹, Vladimir M. Cvetković⁸⁰

Abstract: The rapid proliferation of Artificial Intelligence (AI) and autonomous systems has largely been debated within the paradigms of national defence (Theme 3) and state surveillance (Theme 3.2). However, a critical and underexplored frontier is emerging: the application of these same "dual-use" technologies to the domain of environmental security. This paper addresses the significant ethical and regulatory gap that exists as autonomous systems—such as AI-powered drones, unattended ground sensors, and predictive algorithms— are increasingly repurposed from military and police applications to combat complex environmental threats. This paper builds directly upon the author's foundational research into the theoretical, normative, and institutional frameworks of environmental security (e.g., Ivanov, 2017; Ivanov, 2013). Using a conceptual-philosophical and comparative legal analysis, the research extends this existing "philosophy of environmental protection" beyond the battlefield to address the novel questions posed by AI:

What are the justifiable limits of human control when an autonomous system is tasked with protecting natural resources versus human life?

How do we mitigate algorithmic bias when AI is used to predict environmental crime hotspots, and what are the implications for local and indigenous populations?

What is the appropriate ethical balance between the need for mass surveillance for conservation and the right to privacy?

The paper concludes by asserting the urgent need for a sui generis governance framework tailored specifically for AI in environmental security. It provides strategic recommendations for policymakers and security stakeholders to ensure

⁷⁸ Faculty of Security – Skopje, University "St. Kliment Ohridski" – Bitola, North Macedonia

⁷⁹ Faculty of Security – Skopje, University "St. Kliment Ohridski" – Bitola, North Macedonia

⁸⁰ Faculty of Security Studies, University of Belgrade, Serbia, and Scientific and Professional Society for Risk Management, Belgrade, Serbia

the responsible and ethical deployment of AI, aligning technological capability with long-term ecological stewardship.

Keywords: Artificial Intelligence (AI), Environmental Security, Ethics, Autonomous Systems, Governance, Dual-Use Technology, Resource Protection, Philosophy of Environmental Protection.

INVISIBLE THREATS: LOOKING BACK TO MOVE FORWARD WITH AI- THE MULTIDIMENSIONAL IMPACT OF AI ON ORGANIZATIONAL SECURITY AND HUMAN AGENCY

Tatjana Jovanovic⁸¹

Abstract: As artificial intelligence systems increasingly permeate all domains of human activity – from healthcare and education to employment and governance – new forms of security risks emerge, many of which remain insufficiently recognized. This paper explores the multidimensional infiltration of AI into socio-organizational systems, analysing not only the technological risks, but also the psychological, organizational, and epistemological threats posed by unchecked automation and opaque algorithmic decision-making. Drawing from human resource management (HRM) practices in digitally transformed organizations, the paper identifies early warning signals of AI misuse: diminished human agency, erosion of professional autonomy, over-reliance on predictive analytics, and loss of trust among stakeholders. By extending these findings, the study outlines future development scenarios, ranging from responsible integration of AI grounded in stakeholder dialogue to dystopian trajectories marked by dehumanization and social fragmentation. The final section presents strategic recommendations for promoting responsible AI use, emphasizing the need for transdisciplinary education, critical digital literacy, and anticipatory governance. In shaping the next generation of experts, the role of academia and research institutions becomes vital in embedding ethical reflexivity, systemic thinking, and human-centric values into the very design of AI-driven futures.

Keywords: artificial intelligence, human security, responsible AI

⁸¹ School of Engineering Management, “Union - Nikola Tesla” University, Belgrade, Serbia

APPLICATION OF ARTIFICIAL INTELLIGENCE IN MANAGING OPERATIONAL AND INFORMATION SECURITY RISKS IN SMART MANUFACTURING SYSTEMS

Haris Bajrović⁸², Milan Kovačević⁸³, Predrag Tončev⁸⁴, Nenad Jevtić⁸⁵

Abstract: The paper examines how artificial intelligence (AI) can support the management of operational and information security risks in smart manufacturing systems. It first outlines the convergence of OT and IT environments in Industry 4.0 and the resulting expansion of the attack surface, including cyber-physical vulnerabilities, human error and data integrity issues. The study then analyses key AI approaches—machine learning, deep learning and anomaly detection—for threat prediction, early incident detection and decision support in risk mitigation. Particular attention is paid to integration with existing risk management frameworks, interoperability with legacy equipment and challenges related to data quality, model transparency and adversarial manipulation. Based on a critical review of recent research and pilot implementations, the paper identifies realistic benefits and limitations of AI-enabled security monitoring and proposes guidelines for their responsible deployment in smart factories, emphasising the need for human oversight, explainability and continuous performance evaluation across technical, organisational and regulatory dimensions.

Keywords: smart manufacturing; risk management; anomaly detection; predictive security.

⁸² School of Engineering Management, “Union - Nikola Tesla” University, Belgrade, Serbia

⁸³ School of Engineering Management, “Union - Nikola Tesla” University, Belgrade, Serbia

⁸⁴ School of Engineering Management, “Union - Nikola Tesla” University, Belgrade, Serbia

⁸⁵ School of Engineering Management, “Union - Nikola Tesla” University, Belgrade, Serbia

MACHINE LEARNING–BASED ANOMALY DETECTION FOR OPERATIONAL AND CYBERSECURITY RISK MANAGEMENT IN INDUSTRY 4.0 SYSTEMS

Predrag Tončev⁸⁶, Haris Bajrović⁸⁷, Nenad Jevtić⁸⁸, Milan Kovačević⁸⁹

Abstract: The paper investigates how machine learning–based anomaly detection can enhance operational and cybersecurity risk management in Industry 4.0 systems. It first outlines how the integration of cyber-physical production, IoT connectivity and legacy OT devices expands the attack surface and creates new failure modes on the shop floor. The study then reviews supervised, unsupervised and hybrid anomaly detection techniques for monitoring process data, network traffic and user behaviour in real time. Particular emphasis is placed on early warning capabilities, reduction of false positives and integration with existing risk management and incident-response workflows. Drawing on recent empirical studies and illustrative use cases, the paper identifies key implementation challenges, including data quality, model drift, explainability and adversarial manipulation. Finally, it proposes a set of design principles for deploying ML-based anomaly detection responsibly in smart factories, highlighting the need for human oversight, continuous validation and alignment with organisational and regulatory requirements.

Keywords: machine learning; cyber-physical systems; anomaly detection; operational risk.

⁸⁶ School of Engineering Management, “Union - Nikola Tesla” University, Belgrade, Serbia

⁸⁷ School of Engineering Management, “Union - Nikola Tesla” University, Belgrade, Serbia

⁸⁸ School of Engineering Management, “Union - Nikola Tesla” University, Belgrade, Serbia

⁸⁹ School of Engineering Management, “Union - Nikola Tesla” University, Belgrade, Serbia

DESIGNING SECURE SMART MANUFACTURING: AN ARTIFICIAL INTELLIGENCE APPROACH TO OPERATIONAL AND INFORMATION SECURITY RISKS

Milan Kovačević⁹⁰, Haris Bajrović⁹¹, Predrag Tončev⁹², Nenad Jevtić⁹³

Abstract: The paper analyses how artificial intelligence can contribute to the design of secure smart manufacturing systems while avoiding unrealistic expectations about full automation of security. It first outlines how the convergence of information technology and operational technology, IIoT connectivity, and legacy equipment increases the attack surface and amplifies systemic operational risks. The study then reviews key AI techniques – machine learning, deep learning, and knowledge-based systems – for anomaly detection, predictive maintenance, incident triage, and decision support in risk assessment. Particular attention is paid to integrating these tools into existing management systems, security operation centres, and safety procedures rather than treating AI as a stand-alone solution. Drawing on recent case studies and critical literature, the paper identifies persistent challenges related to data quality, explainability, adversarial manipulation, organisational readiness, and regulatory compliance. Finally, it proposes practical design principles for socio-technical implementation of AI in smart factories, emphasising human oversight, gradual deployment, continuous validation, and explicit allocation of responsibility for AI-supported security decisions. The aim is not to promise risk elimination, but to clarify where AI demonstrably improves detection and response, where it also shifts risks, and where it introduces new vulnerabilities.

Keywords: human oversight; decision responsibility; anomaly detection; predictive maintenance.

⁹⁰ School of Engineering Management, “Union - Nikola Tesla” University, Belgrade, Serbia

⁹¹ School of Engineering Management, “Union - Nikola Tesla” University, Belgrade, Serbia

⁹² School of Engineering Management, “Union - Nikola Tesla” University, Belgrade, Serbia

⁹³ School of Engineering Management, “Union - Nikola Tesla” University, Belgrade, Serbia

QUALITY ASSURANCE IN HIGHER EDUCATION IN THE ERA OF THE MASS ADOPTION OF ARTIFICIAL INTELLIGENCE SOFTWARE PACKAGES

Nikola Živković⁹⁴

Abstract: The rapid adoption of generative artificial intelligence in higher education has introduced a range of regulatory and accreditation challenges, particularly in the development of curricula and study programs. While AI-based tools may contribute to efficiency and standardization in curriculum design, their uncontrolled use poses risks related to superficial content, lack of contextual relevance, and the erosion of academic autonomy and educational quality. In this context, national accreditation bodies are increasingly required to develop mechanisms for identifying and evaluating curricula that are fully or partially generated using artificial intelligence. This paper analyzes key indicators that may signal AI-generated curricula, including structural uniformity, generic terminology, the absence of institutional and national context, and inconsistencies between learning outcomes, teaching methods, and assessment systems. Special emphasis is placed on the role of expert evaluation committees, the integration of qualitative academic review with digital tools for AI-text detection, and the necessity of establishing clear guidelines and ethical frameworks within accreditation procedures. The aim of the paper is to provide practical recommendations for national accreditation bodies in the Republic of Serbia, supporting the preservation of quality, transparency, and academic integrity in the era of artificial intelligence.

Keywords: artificial intelligence, educational quality, academic integrity, education regulation

⁹⁴ National Accreditation Body of the Republic of Serbia, Belgrade, Serbia

Concluding Remarks

Dear colleagues, distinguished guests, and participants,

As we conclude the International Scientific-Professional Conference "Artificial Intelligence and Security in the XXI Century," held on November 19, 2025, at the School of Engineering Management, "Union-Nikola Tesla" University, I find myself reflecting on the extraordinary intellectual journey we have shared throughout this day. What began this morning as a gathering of scholars and practitioners from sixteen countries across four continents has evolved into something far more significant—a community of shared purpose, united by our commitment to ensuring that artificial intelligence serves humanity's highest aspirations rather than amplifying our vulnerabilities. The forty-five presentations we have witnessed today represent more than academic contributions; they constitute a collective map of the challenges and opportunities that define our digital era. From the philosophical dimensions of intercultural AI ethics to the technical intricacies of preventing data leakage into large language models, from the geopolitical implications of AI competition to the intimate questions of trust in AI-enabled healthcare—we have traversed the full spectrum of concerns that shape security in the 21st century.

Several themes have emerged with particular clarity throughout our discussions. First, the recognition that AI has fundamentally transformed the concept of security itself—from reactive defence to predictive anticipation, from physical protection to algorithmic sovereignty, from territorial control to information governance.

Second, the understanding that technological capability must be balanced with ethical responsibility, transparency, and human oversight. And third, the acknowledgment that no single nation, institution, or discipline possesses all the answers—meaningful progress requires exactly the kind of international, interdisciplinary collaboration we have practiced here today.

Our keynote speakers—Dean Prof. Dr. Vladimir Tomašević, COO AikBank Maja Mikić, ISAC Fund Director Nikola Petrović, and Prof. Dr. Duško Tomić—have provided us with frameworks that bridge theory and practice, reminding us that AI security is simultaneously a technological challenge, an ethical imperative, a governance necessity, and a profoundly human concern. Their insights have set

the intellectual tone for discussions that ranged from the governance of autonomous weapons systems to the role of AI in education, from cybersecurity resilience to the protection of critical infrastructure.

Thematic panels—covering AI regulation and ethics, military and defence applications, cybersecurity and hybrid threats, critical infrastructure protection, education and higher learning, healthcare and diagnostics, smart cities and public safety, and data privacy and protection—have demonstrated the extraordinary breadth and depth of expertise assembled here. Each presentation has contributed a crucial piece to the larger puzzle of how we govern, deploy, and live alongside artificial intelligence in ways that enhance rather than undermine our collective security.

I am particularly struck by the quality of engagement throughout the day—the probing questions, the thoughtful challenges, the constructive dialogue that has characterized our interactions. This is precisely the kind of intellectual discourse that advances knowledge and shapes policy. The conversations that began in our modest conference room will continue in your research, in your institutions, in policy discussions, and in the practical decisions that will define the security landscape for generations to come.

I want to express my deepest gratitude to all who made this conference possible. To our Scientific Committee, whose expertise and guidance ensured the academic excellence of our program. To our keynote speakers, who shared invaluable insights from both theoretical and practical perspectives. To every presenter, whose rigorous scholarship and practical wisdom have enriched our collective understanding. To our organising committee colleagues—Dr. Ana Jurčić, Dr. Milena Cvjetković, Dr. Damir Ilić, MSc Luka Latinović and MSc Olga Mašić—whose tireless efforts transformed vision into reality. And to each participant, whose presence, engagement, and contributions have made this gathering truly international in scope and impact.

The work we have begun here today does not end with the closing of this conference. The challenges we have identified require sustained attention, the solutions we have proposed demand rigorous testing, and the collaborations we have initiated need continued nurturing. I encourage you to maintain the connections formed here, to pursue the research directions suggested by our discussions, and to translate the insights gained into concrete action within your

respective spheres of influence.

At your respective universities, research centres, agencies, and organizations worldwide, bring forward not just the knowledge we have shared, but the collaborative spirit that has brought this gathering to life. Let us continue to work together—across borders, disciplines, and sectors—to ensure that the integration of artificial intelligence into our security systems is guided by wisdom, constrained by ethics, and directed toward the enhancement of human dignity and collective wellbeing.

The future of AI and security will be written not by technology alone, but by the choices we make, the values we uphold, and the governance frameworks we construct. Today, we have taken an important step in shaping that future. Let us continue this vital work with the same rigor, responsibility, and collaborative spirit that has characterized this conference.

Thank you for your participation, your insights, and your commitment to addressing one of the most consequential challenges of our time. May the knowledge we have shared and the relationships we have built serve as foundations for continued progress toward a secure, ethical, and human-centered future in the age of artificial intelligence.

I look forward to our continued collaboration in the months and years ahead.

Dr. Katarina Štrbac

Full Professor

Conference Organiser and Editor

School of Engineering Management, "Union-Nikola Tesla" University, Belgrade, Serbia

CIP - Каталогизација у публикацији
Народна библиотека Србије, Београд

351.861(048)

004.8(048)

327.56:351.861(048)

INTERNATIONAL Scientific-professional Conference
Artificial intelligence and security in the XXI Century
(2025 ; Belgrade) Book of Abstracts / International
Scientific-professional Conference Artificial intelligence
and security in the XXI Century, November 19, 2025;
Conference organiser School of Engineering Management,
University "Union - Nikola Tesla", Belgrade, Republic of
Serbia;

(Ed.). Katarina Štrbac

- Belgrade : School of Engineering Management, :
University "Union-Nikola Tesla ; Slovakia : European
Institute of Further Education,
2025 (Belgrade : Black and White). - [87] str. ; 25 cm
Tiraž 100.

ISBN 978-86-89691-45-0 (SEM)

ISBN 978-80-89926-24-4 (EIFE)

а) Национална безбедност -- Стратешки аспект --
Апстракти б) Вештачка
интелигенција -- Апстракти

COBISS.SR-ID 182028297

ABOUT THE CONFERENCE

The International Scientific-Professional Conference on **Artificial Intelligence and Security in the XXI Century** brings together leading researchers, practitioners, and policymakers to discuss the latest advances, challenges, and future directions in AI and cybersecurity.

This Book of Abstracts contains contributions from distinguished experts across multiple domains, addressing critical topics including machine learning, cryptography, privacy-preserving technologies, biometric systems, and the intersection of artificial intelligence with security systems.

CONFERENCE DETAILS

Date

November 19, 2025

Venue

Belgrade, Serbia

Format

Hybrid: In-person and Online

School of Engineering Management

"Union-Nikola Tesla" University

Belgrade, Serbia
