INTERNATIONAL CONFERENCE

NEW AND EMERGING TECHNOLOGIES IN DEFENCE EDUCATION, TRAINING AND GOVERNANCE

The international conference on New and Emerging Technologies in Defence Education, Training and Governance is held under the auspices of Security and Defence Quarterly, and is organised by the Doctoral School of the War Studies University (Poland) and MIT University Skopje (North Macedonia), in cooperation with Pamukkale University (Turkey), Rzeszow University of Technology, the Faculty of Electronics, Telecommunications and Informatics at Gdańsk University of Technology (Poland), and the Faculty of Management and Command of the War Studies University (Poland).

21 May 2026

Microsoft Teams

9.00 – 10.30 (CEST, Warsaw time) **Conference opening**

Link: https://tinyurl.com/3f8sa429

Col. Prof. Tadeusz Zieliński, War Studies University, Poland

Prof. Katerina Veljanovska Blazhevska, MIT University, Skopje, North Macedonia

Keynote speakers

Prof. Peter Holowka, University of Calgary & West Point Grey Academy, Canada, *Key Global Considerations for AI and Educational Technology Adoption Within Military and Civilian Contexts*

Prof. Monika Wolfmayr, Jamk University of Applied Sciences, Finland, *Algorithms and Methods for Cybersecurity of Critical Infrastructures in Quantum Computing*

10:30 – 12:30 (Central European Summer Time)		
Panel 1: AI-Driven Defence Training and Immersive Simulation Systems **Link: https://tinyurl.com/3f8sa429** **Chair: prof. Michael Knott,** University of Namibia, **Dawid Trela, Msc** War Studies University, Poland	**Panel 2: Unmanned Systems, U-Space Integration and UAV Operational Innovation.** **Link: https://tinyurl.com/3y74t85m** **Chair: prof. Marinel-Adi Mustata**, Carol I National Defence University, Romania, **Martyna Łuszczek,** War Studies University, Poland	**Panel 3: Disinformation, Cognitive Security and Societal Resilience** **Link: https://tinyurl.com/2728ekdy** **Chair: prof. Thomas W. Friis,** University of Southern Denmark, **Patryk Michałkiewicz, MSc** War Studies University, Poland
Danielle Ayomide Jesudamilare Awonusi, Hong Kong Chu Hai College of Higher Education, Hong Kong, *AI Enhanced Defence Training and Ethical Governance: Lessons for Emerging and Hybrid Security Contexts* **prof. Małgorzata Gawlik- Kobylińska**, War Studies University, Poland, *Four-Dimensional Instructional Design for Immersive Defence Training: Integrating Cognitive, Emotional, Social, and Psychomotor Dimensions* **dr Agnieszka Bekisz,** Military University of Land Forces, *Artificial Intelligence as a Tool Supporting Risk Management in Defense Training* **Kamil Jan Margielewicz**, **MSc** University of Economics in Katowice and Upper Silesian University named after Wojciech Korfanty in Katowice, *Artificial Intelligence as an element of educating Polish uniformed services personnel in the realities of cyberterrorist threats*	**prof. Peter Cumpson**, Auto617 Ltd (UK), United Kingdom, *Detection-Triggered Dispersion in UAV Swarms: Implications for Defence Training, Counter-UAS Doctrine, and Emerging Directed-Energy Threats* **Arkadiusz Olejarz**, **MSc** War Studies University, Poland, *The Use of Drones for Airport Infrastructure Inspection in the Context of U Space Implementation* **Rafał Lipka-Kadaj, MSc** Civil servant, Poland, *Civilian Drone Operators and the Development of Drones in the Polish Army* **Dominika Przybylska,** Kozminski University, Poland, *Legal liability for autonomous system failures during the training of mini and micro UAV operators* **Andrada Petrescu, "**Nicolae Balcescu**"** Land Forces Academy of Sibiu, *Technical University of Cluj-Napoca, Romania, Military image restoration by morphological-based dehazing algorithms*	**prof. Weronika Jakubczak**, Fire University, Poland, *Immersive and Simulation Technologies in Developing Independent Thinking and Societal Resilience against Hybrid Threats under Conditions of High Uncertainty* **PhDr. Tomáš Kolomazník** Metropolitan University Prague, Czech Republic, *Tools for combating disinformation in the public sphere in the age of artificial intelligence* **Krzysztof Zieliński**, **PhD** War Study University, Poland, *Social resilience and local crisis preparedness* **Wojciech Sługocki**, **PhD** Academy of Applied Sciences in Wrocław, Poland, *Rethinking Education in the New Infosphere: Systemic Responses to the Age of Disinformation* **Eng. Monika Zamłyńska**, Military University of Land Forces, *A model for cybersecurity competence development based on virtual environments and simulation driven learning* **prof. Katerina Veljanovska Blazhevska**, MIT University Skopje, North Macedonia, **prof. Dorota**

Piotr Wójtowicz, MSc War Studies University, **Dawid Trela, MSc** War Studies University, *Between Confidentiality and Cooperation: Cyber Threat Intelligence Sharing under Article 45 DORA in the AML/CFT Perspective* **Nathan Patrick-Lecki**, University of Warsaw, Poland, *Integrating Artificial Intelligence into Simulation-Based Training for Crisis Management*	**Justyna Małysiak, PhD** Military University of Land Forces, Poland, **Piotr Wojnarowicz MA** University of Wrocław, Poland *Management of the competency capital of civil and military structures representatives as a factor determining the effectiveness of response in crisis situations – a contribution to research*	**Domalewska,** War Studies University, Poland, **Piotr Okulski, MSc,** War Studies University, Poland, *Visual disinformation in social media: challenges and implications for education*

12:30 – 14:30 (Central European Summer Time)	
Panel 4: Legal and Regulatory Challenges of Emerging Defence Technologies **Link: https://tinyurl.com/3f8sa429** **Chair: prof. Ruslana Grosu,** Armed Forces Military Academy "Alexandru cel Bun" in Chisinau, Moldova, **Agnieszka Bekisz, PhD** Military University of Land Forces, **Przemysław Gasztold, PhD** War Studies University, Poland	**Panel 5: Hybrid Threats, Strategic Governance and Critical Infrastructure Security** **Link: https://tinyurl.com/3y74t85m** **Chair: prof. Marco Marsili**, University of Lisbon, Portugal, **Karolina Mikusek, MA** War Studies University, Poland
Karol Chaberka, MSc University of Economics in Katowice, Poland, *From Visualization to Behavioural Change: Immersive Technologies as Instruments for Environmental ESG KPI Measurement and Governance in Defence and Security Contexts* **Eng Kacper Zdrojewski**, **MSc** War Studies University, Poland, *Preparing for Algorithmic Warfare: Immersive Learning, Human-in-the-Loop, and Regulatory Challenges* **Jan Szych**, University of Warsaw, Poland, *Fiscal engineering as a governance tool in technology-driven security systems: balancing efficiency and fundamental rights*	**prof. Weronika Jakubczak**, Fire University, Poland, *Cyber Education for Security in the IoT and IoE Ecosystem: Immersive Technologies for Building Cyber Resilience in Hybrid Conflicts* **CDR Krzysztof Pająk**, **PhD** War Study University, Poland War Study University, Poland, *'No Boots on the Ground': Challenges and Implications of Removing Human Presence from Military Doctrine and Operations* **Lieut. Cmdr. George Margaros,** Hellenic Navy, *Quantitative Decision Study on the Integration of Nuclear Energy into a Country* **Achille Castrogiovanni**, **PhD** University of Sunderland, United Kingdom, *Hybrid Coercion and Maritime Deterrence in the Baltic Sea: Critical Undersea Infrastructure and Narrative Contestation*

Anna Stawińska, Cardinal Stefan Wyszyński University, Poland, *Legal and Economic Determinants of Implementing Immersive Technologies in Defence Training Systems - Institutional and Market Perspective* **Andrzej Kozik**, University of Gdańsk, Poland, *Regulating the Smart Threat: Legal and Governance Challenges in Restricting Foreign Connected Devices in the Context of National Security* **Ignacy Klajbor**, University of Gdańsk, Poland, *Legal Frameworks and Regulatory Challenges in the Implementation of Artificial Intelligence in Immersive Defence Training Systems*	**Jari Hautamäki PhL**, Jyväskylä University/Jyväskylä University of Applied Sciences, *Cybersecurity Intelligence Sharing Model* **Pedro Silva Baptista**, Minho University, Portugal, *Epistemic Sovereignty in the Battlespace: Human Capital and the Governance of Emerging Defense Technologies in African States* **Joanna Pastuszak-Cybulska, MsC** University of the National Education Commission in Krakow *From exclusion to inclusion: addressing the challenges of alerting deaf people to danger*

14:30-15:00 **Conference Closing**

(Central European Summer Time) **Link: https://tinyurl.com/3f8sa429**

Keynote speaker:

prof. Bert Chapman, Purdue University, United States – *Artificial Intelligence in the Curriculum of U.S. Professional Military Educational Institutions*

SECURITY & DEFENCE QUARTERLY

QR CODES

Opening & closing session, Panel I & IV

Panel II & V

Panel III

POLITECHNIKA GDAŃSKA | WYDZIAŁ ELEKTRONIKI, TELEKOMUNIKACJI I INFORMATYKI

ARGON World leaders in CBRN/ HazMat training systems

SZKOŁA DOKTORSKA Akademii Sztuki Wojennej

МИТ УНИВЕРЗИТЕТ

POLITECHNIKA RZESZOWSKA im. IGNACEGO ŁUKASIEWICZA

Integra AV Audio Video & Virtual Reality

megmar logistics & consulting

INTERNATIONAL CONFRERENCE

NEW AND EMERGING TECHNOLOGIES IN DEFENCE EDUCATION, TRAINING AND GOVERNANCE

CONFERENCE ABSTRACTS BOOK

Keynote speakers

Link: https://tinyurl.com/3f8sa429

Prof. Peter Holowka, University of Calgary & West Point Grey Academy, Canada, *Key Global Considerations for AI and Educational Technology Adoption Within Military and Civilian Contexts*

Abstract:

Education, whether in a military or civilian context, has transformed significantly in recent decades. Computer use within institutions of learning has shifted from a peripheral novelty to an essential pedagogical and operational infrastructure. The emergence of Artificial Intelligence (AI) into the mainstream of society and education is a furtherance of this trend of digital transformation. This presentation addresses the key considerations leaders in all industries must evaluate when planning for and implementing new technologies, including AI. This presentation is rooted in organizational innovation adoption research conducted within a Canadian context of 2.2+ million square kilometres, affecting 1.14+ million students—the largest study of its kind ever conducted. In addition to the binding legal considerations of AI use, determined by the landmark European Union Artificial Intelligence Act, leaders must be similarly attentive to more nuanced and less clearly defined challenges, such as financial viability and stakeholder perceptions. The interconnected nature of global financial markets, widespread cultural influences, and the Brussels Effect all make these considerations universal rather than purely regional phenomena. This paper explores the complex global issues relating to AI governance and strategy, applicable to military and non-military organizations alike. These foundational and structural topics will continue to have an increasing impact on instructional approaches, institutional resilience, and public sentiment within the defence sector and beyond.

Keywords:

AI Governance, Education, EU AI Act, Organizational Innovation Adoption

Prof. Monika Wolfmayr, Jamk University of Applied Sciences, Finland, *Algorithms and Methods for Cybersecurity of Critical Infrastructures in Quantum Computing*

Abstract:

Information technology is vital in handling critical infrastructures such as power grids, water supplies, healthcare, transportation networks, and infrastructures in space. Quantum computing has potential to revolutionize critical

infrastructures by enabling faster optimization, simulation and data analysis for complex systems. The adoption of quantum technologies demands the reconsideration of cybersecurity protocols to mitigate quantum-era threats. Along with the technological progress in quantum computing, there is a risk of cyberattacks leading to research questions asking what new quantum computing algorithms are being designed to secure critical infrastructures, how they compare to conventional methods, how quantum computing algorithms are being designed to enhance the reliability of critical infrastructures and what quantum computing methods are emerging for ensuring the stability and accuracy of computations critical to infrastructure management. This work focuses on answering those research questions by presenting a scoping review conducted considering 420 research articles. The scoping review shows the possibilities that can be achieved by implementing various algorithms and methods for cybersecurity. The study encircles many categories such as optimization, security, networking, algorithms, protocols, communication, power systems, and space science, and shows that quantum computing can enhance their protection. This study discusses techniques for the cybersecurity of critical infrastructures in quantum computing and presents results on infrastructure analysis. We targeted various research phrases regarding the research questions mentioned about algorithms and methods for cybersecurity of critical infrastructure in quantum computing. This work compels the reader to consider the various ways critical infrastructures can be protected from different threats including cyberattacks.

Keywords:

Quantum Computing, Cybersecurity, Quantum Computing Applications, Quantum Algorithms, Critical Infrastructures

PANEL 1

Link: https://tinyurl.com/3f8sa429

AI-Driven Defence Training and Immersive Simulation Systems

1. **Danielle Ayomide Jesudamilare Awonusi**, Hong Kong Chu Hai College of Higher Education, Hong Kong,
   AI Enhanced Defence Training and Ethical Governance: Lessons for Emerging and Hybrid Security Contexts

   Abstract:

   As artificial intelligence and immersive technologies increasingly shape defence education and training, they also reconfigure questions of power, accountability and institutional resilience. This paper examines how AI enhanced training environments, including simulation, decision support systems and data driven assessment tools, affect governance practices in defence and security institutions, with particular attention to emerging and hybrid security contexts. The analysis proceeds in three steps. First, it maps key uses of AI and immersive systems in defence education and training, focusing on how they promise to improve preparedness, scenario complexity and individualised learning. Second, it identifies ethical and governance challenges that arise from these deployments, including opacity in algorithmic decision support, unequal access to advanced training infrastructures, and risks of cognitive overload or manipulation. Third, it considers what lessons can be drawn for institutions in the Global South and in hybrid security environments, where resource constraints, external technological dependence and contested political legitimacy shape the adoption of new technologies. Drawing on documentary analysis and recent policy debates on AI governance and digital sovereignty, the paper argues that AI enhanced defence training must be embedded in robust frameworks of ethical oversight, transparency and institutional learning. It concludes by outlining principles for aligning technological innovation in defence education with democratic accountability, human rights and long term societal resilience.

   Keywords:

   AI governance; defence education; immersive training; digital sovereignty; Global South

2. **prof. Małgorzata Gawlik- Kobylińska**, War Studies University, Poland, *Four-Dimensional Instructional Design for Immersive Defence Training: Integrating Cognitive, Emotional, Social, and Psychomotor Dimensions*

Abstract:

Rapid integration of immersive technologies into defence education and training is transforming the design of simulation-based learning, particularly in contexts that require high levels of operational readiness. Virtual reality (VR), augmented reality (AR), and CAVE (Cave Automatic Virtual Environment) systems enable advanced experiential learning; however, instructional approaches remain uneven, with a dominant focus on cognitive outcomes and limited integration of other learning dimensions. Four-Dimensional Instructional Design (4D ID) is introduced as a framework for structuring immersive defence training in a more balanced and operationally relevant way. The model integrates four interdependent dimensions of learning: cognitive, emotional, social, and psychomotor. Evidence is drawn from a structured review of immersive learning literature, complemented by conceptual modelling and scenario-based analysis tailored to CAVE-supported environments. Results indicate a persistent imbalance in the representation of learning dimensions. Psychomotor competencies—critical for performance in high-risk and crisis situations—emerge as a distinct yet systematically underdeveloped component of current training designs. Addressing this gap, a set of scenario design guidelines is proposed, emphasising embodied interaction, coordinated team performance, and decision-making under conditions of stress and uncertainty. Application of the 4D ID framework supports closer alignment between immersive technologies and operational training requirements. Implications extend to improving the effectiveness, realism, and resilience of defence education and training systems.

Keywords:

immersive technologies; defence training; instructional design; 4D ID; psychomotor domain; simulation-based learning; embodied cognition; training effectiveness; learning

3. **dr Agnieszka Bekisz,** Military University of Land Forces, Poland, *Artificial Intelligence as a Tool Supporting Risk Management in Defense Training*

Abstract:

The article identifies the key benefits resulting from the use of AI, including increased effectiveness of risk identification, the development of decision-making competencies, and the possibility of conducting training in conditions similar to real crisis situations. At the same time, it highlights the emergence of new threats related to the use of AI, such as algorithmic errors, the risk of cyberattacks, ethical concerns, and the lack of transparency in decision-making processes. At the same time, new threats related to the use of AI will be highlighted, such as algorithmic errors, the risk of cyberattacks, ethical issues, and the lack of transparency in decision-making processes.

Keywords:

AI, crisis management, cybersecurity, decision-making processes, risk identification, simulation-based training

4. **Kamil Jan Margielewicz**, **MSc** University of Economics in Katowice and Upper Silesian University named after Wojciech Korfanty in Katowice, *Artificial Intelligence as an element of educating Polish uniformed services personnel in the realities of cyberterrorist threats*

Abstract:

In my presentation, I would like to present issues related to artificial intelligence, broadly defined, in the context of the education of Polish uniformed services personnel. I am leaning towards this topic due to my own research interest in the subject, the current global geopolitical situation, and to engage other researchers. I will present specific examples of real-world applications and the potential of AI in training personnel from specific uniformed services of the Third Polish Republic. The essence of the presentation is to demonstrate the importance of AI in the context of cardinal education, particularly in terms of cyber threats and cyberterrorism in the broadest sense. In a few final sentences, I will also mention the possibilities of international cooperation – in terms of countering cyberterrorism – using AI. The topic was developed based on library and archival research, the author's knowledge and experience in the subject area, and selected statements from experts and specialists in the field.

Keywords:

Artificial intelligence, military, cyberterrorism, technology

5. **Piotr Wójtowicz, MSc** War Studies University, **Dawid Trela, MSc** War Studies University, *Between Confidentiality and Cooperation: Cyber Threat Intelligence Sharing under Article 45 DORA in the AML/CFT Perspective*

Abstract:

The presentation addresses the sharing of cyber threat intelligence (CTI) within the financial sector under Article 45 of the DORA Regulation, examined from the perspective of the anti-money laundering and counter-terrorist financing (AML/CFT) framework. It begins with a normative reconstruction of Article 45 as a sector-specific regime for CTI sharing, situated within the broader architecture of ICT risk management, incident reporting obligations, and the relationship between DORA and the NIS2 Directive. The presentation then discusses the cumulative conditions for the lawful exchange of information, arising from data protection law, the protection of legally privileged information, and competition law constraints. Against this background, it develops a functional analysis of how CTI may be operationalised within AML/CFT processes, particularly in risk assessment models, transaction monitoring scenarios, and procedures leading to the submission of suspicious transaction/activity reports (STR/SAR), while respecting key limitations such as the prohibition of tipping-off and the need to preserve the integrity of reporting channels to financial intelligence units (FIUs). The presentation also considers the potential role of supervisory authorities and the Polish financial intelligence unit (the General Inspector of Financial Information – GIIF) within CTI-sharing arrangements established under Article 45 DORA, with reference to emerging national supervisory practice. It concludes by outlining selected de lege ferenda proposals concerning the integration of CTI into the AML/CFT framework. The overall aim of the presentation is to demonstrate that Article 45 DORA may function as a regulatory nexus between the cyber resilience regime and the AML/CFT system, and to identify the conditions under which such integration can be both legally permissible and operationally effective.

Keywords:

Digital Operational Resilience Act (DORA); cybersecurity; Cyber Threat Intelligence (CTI); information sharing; AML/CFT; financial intelligence unit (FIU); financial sector

6. **Nathan Patrick-Lecki**, University of Warsaw, Poland, *Integrating Artificial Intelligence into Simulation-Based Training for Crisis Management*

Abstract:

The increasing complexity of crisis environments necessitates more adaptive and data-driven training approaches. This study investigates the integration of Artificial Intelligence (AI) into simulation-based training systems for crisis management, with a particular focus on enhancing decision-making under dynamic and high-pressure conditions. The paper analyses selected AI-driven solutions, including intelligent agents, scenario generation algorithms, and predictive analytics, applied in simulation environments such as VR-based crisis response training and CBRN incident simulations. It examines how AI enables real-time adaptation of scenarios based on trainee performance, allowing for personalised learning pathways and more realistic representation of evolving threats. Methodologically, the study is based on a qualitative analysis of existing AI-supported training platforms and selected case studies from defence and emergency response sectors. The paper evaluates the impact of AI integration on key training outcomes, including situational awareness, response time, and decision accuracy. Additionally, the study addresses critical challenges related to AI implementation, such as data quality, system transparency, and ethical considerations in automated decision-support systems. The findings highlight that while AI significantly enhances training realism and effectiveness, its successful adoption requires robust governance frameworks and human oversight.

Keywords:

Artificial Intelligence; Simulation-Based Training; Crisis Management; Defence Education; Decision-Making; Adaptive Learning

PANEL 2

Link: https://tinyurl.com/3y74t85m

Unmanned Systems, U-Space Integration and UAV Operational Innovation

1. **prof. Peter Cumpson**, Auto617 Ltd (UK), United Kingdom, *Detection-Triggered Dispersion in UAV Swarms: Implications for Defence Training, Counter-UAS Doctrine, and Emerging Directed-Energy Threats*

Abstract:

High-power microwave (HPM) systems are increasingly presented as effective counter-swarm weapons because a single emission may disable multiple uncrewed aerial vehicles (UAVs). This paper argues that such weapons also possess an intrinsic weakness of direct relevance to defence education, training, and operational doctrine: an HPM emission sufficient to affect one UAV is likely to be detectable by others, thereby triggering rapid autonomous dispersion and reducing the effectiveness of subsequent engagements. Using a lightweight threshold detector based on a neon discharge element as an illustrative warning device, the study develops an analytical and Bayesian stochastic model linking first-pulse kill probability, swarm geometry, warning time, and lateral evasion dynamics to follow-up re-engagement outcomes. The analysis introduces the concept of a "Vanguard UAV," a sacrificial forward platform intended to provoke the initial HPM emission and create a tactically valuable dispersion interval for the main swarm. Results suggest that unless near-unity first-pulse lethality is achieved, even simple detection and dispersal behaviours can reduce re-engagement opportunities by more than an order of magnitude. The paper highlights implications not only for counter-UAS technology assessment, but also for wargaming, doctrinal development, simulation-based training, and the teaching of adaptive human-machine tactics in emerging defence environments.

Keywords:

UAV, DEW, HPM, High Power Microwaves, Movement to Contact

2. **Arkadiusz Olejarz**, **MSc** War Studies University, Poland, *The Use of Drones for Airport Infrastructure Inspection in the Context of U-Space Implementation*

Abstract:

The increasing adoption of unmanned aerial systems (UAS) in civil aviation has opened new opportunities for enhancing airport operations, particularly in the field of infrastructure inspection. This article examines the potential of drones to support routine and emergency inspections of airport infrastructure, including runways, taxiways, lighting systems, fencing, and other critical facilities. The study explores how drone based inspection systems can improve operational efficiency, reduce inspection time, and enhance data accuracy compared to traditional manual methods. Special attention is given to the technological capabilities of modern drones, such as high resolution imaging, thermal sensors, and automated flight planning. The analysis is conducted within the regulatory and operational framework of U-Space, the European system designed to enable safe, coordinated, and scalable drone operations in complex airspace environments. The article discusses how U-Space services—such as network identification, geofencing, flight authorization, and traffic information—can facilitate the safe integration of inspection drones into airport environments, which are characterized by high safety requirements and dense air traffic. Potential challenges, including communication reliability, cybersecurity, and coordination with air traffic control, are also addressed. The findings indicate that drone supported inspections, when combined with U-Space services, can significantly enhance the digitalization and automation of airport operations. The article concludes by outlining recommendations for airport operators, regulators, and technology providers to support the wider adoption of drone based inspection systems in line with emerging European standards.

Keywords:

aviation safety, drones, unmanned aerial systems, U-Space

3. **Rafał Lipka-Kadaj, MSc** Civil servant, Poland, *Civilian Drone Operators and the Development of Drones in the Polish Army*

Abstract:

The approach to the use of drones for military purposes was completely changed by the war in Ukraine. During the war, it was observed that, for example, a tank worth millions of dollars could be disabled at a relatively low cost (an FPV drone with an explosive charge). This fact is important because every war generates significant costs, and in long-term wars, the side that minimizes expenses theoretically has a greater chance of winning. Consequently, an increased demand for unmanned aerial vehicle pilots was observed. The author analyzed the advisability of incorporating civilian drone operators, including gamers, into the Polish Army. Available Polish and international literature was analyzed. The author primarily utilized analytical and synthesis methods and reviewed available sources. As a result, the hypothesis emerged that incorporating civilian drone pilots and gamers into the military is a valid approach to increasing the defensive potential of the Polish Army. In the author's opinion, this topic deserves extensive discussion due to it’s importance (strengthening defense capabilities) and scale (currently drones dominated the battlefield). The purpose of this article is to present the rationale for recruiting civilians (drone pilots, gamers) to enhance the Polish military's potential, given the growing importance of drone use on the battlefield. The author also contrasts the war zones in Ukraine with those in Iraq and Afghanistan.

Keywords:

drone pilots, army, drones, gamers, conflict

4. **Dominika Przybylska,** Kozminski University, Poland, *Legal liability for autonomous system failures during the training of mini and micro UAV operators*

Abstract:

The rapid integration of Artificial Intelligence (AI) and autonomous flight modes in mini and micro Unmanned Aerial Vehicles (UAVs) has transformed military and security training. While these systems significantly reduce the cognitive load on trainees, they introduce complex legal challenges regarding liability. In a high-stakes training environment, the boundary between human error and systemic technical failure is increasingly blurred, creating a regulatory vacuum. This paper examines the legal responsibility for damages or accidents occurring when autonomous sub-systems—such as auto-collision avoidance or path-finding algorithms—fail during instructional sessions. Utilizing a comparative analysis of current aviation laws, military service regulations, and the emerging EU AI Act, the research focuses on three primary dimensions: the instructor's duty of care, product liability versus operational error, and the legal status of the trainee. The analysis argues that current "service pragmatics" are ill-equipped for the era of autonomous training. It proposes a "Distributed Liability Model" for military institutions, emphasizing the need for standardized black-box data logging to provide forensic legal evidence. Ultimately, the transition to autonomous training requires a shift from individual blame to a systemic certification process, ensuring that AI-driven educational tools meet rigorous safety and accountability standards.

Keywords:

UAV Training, Autonomous Systems, Legal Liability, Military Law, AI Act, Mini-UAVs.

5. **Andrada Petrescu,** "Nicolae Balcescu" Land Forces Academy of Sibiu, Technical University of Cluj-Napoca, Romania, Military image restoration by morphological-based dehazing algorithms

Abstract:

The restoration of images affected by fog, smoke and dust (also called dehazing) is a topic of great interest in the field of image processing, due to its applicability in various domains such as transportation and autonomous driving, video surveillance and remote sensing. However, in security and defense scenarios, the discussion goes beyond the mere visual enhancement of images. In military operational environments, images captured by optical sensors can often be affected by smoke, fog or dust. Unlike the common weather conditions, the smoke and dust are harder to remove since they affect non-uniformly the scene. These degradations reduce the contrast and alter the appearance of objects, thus affecting both human interpretation and their automatic detection and recognition by both classical and deep learning computer vision systems. In this context, image dehazing represents a research direction of significant interest, aimed at restoring visual information and improving image quality under reduced-visibility conditions. The current paper provides a morphological processing based framework, implemented in the form of a software application with graphical user interface (GUI) for the restoration of military-specific images, at various degrees upon user's selection. The final objective is to enable the use of the resulting enhanced images in applications such as surveillance, reconnaissance, object detection, and image analysis in order to support the decision-making process. Furthermore, modern methods based on polarized imaging and deep learning, capable of reducing the effects of fog, smoke and dust, will also be discussed.

Keywords:

military image restoration, image dehazing, smoke removal, morphological operators

6. **Justyna Małysiak, PhD** Military University of Land Forces, Poland, **Piotr Wojnarowicz MA** University of Wrocław, Poland *Management of the competency capital of civil and military structures representatives as a factor determining the effectiveness of response in crisis situations – a contribution to research*

Abstract:

In an era of hybrid threats and increasing interdependence of global markets, state resilience depends increasingly on the stability of strategic supply chains. Traditional crisis management training methods are generally based on static scenarios that fail to reflect the dynamic nature of contemporary economic and logistical crises and do not develop the competencies necessary to interpret multidimensional warning signals. This article examines the potential of advanced data analytics, particularly predictive modelling and dependency graphs, as innovative educational tools in both defence and civilian education. The article presents a case study on the application of econometric models and network data analysis for identifying bottlenecks and forecasting the risk of disruptions in the supply of agricultural raw materials of strategic importance to the Central and Eastern European region. It analyses how data analytics tools based on econometric models can support decision-making processes under conditions of limited and contradictory information, which are typical of crisis situations. The article also highlights the regulatory and competency requirements associated with the implementation of predictive algorithms within public management structures, emphasising the need for the systematic development of digital analytical competencies among decision-makers. The retrospective analysis demonstrates that the convergence of market, agronomic, and network indicators generated operationally useful warning signals many months before the escalation of the crisis. These signals, however, were not captured within the existing crisis management procedures. The proposed methodological approach enables a transition from a reactive to a proactive model of crisis management and may constitute an important component of training programmes for both military and civilian institutions, in line with NATO baseline requirements for resilience and national crisis management frameworks.

Keywords:

predictive modelling, crisis management, state resilience, supply chains, defence education, data analytics, dependency graphs, food security

PANEL 3

Link: https://tinyurl.com/2728ekdy

Disinformation, Cognitive Security and Societal Resilience

1. **prof. Weronika Jakubczak**, Fire University, Poland, *Immersive and Simulation Technologies in Developing Independent Thinking and Societal Resilience against Hybrid Threats under Conditions of High Uncertainty*

Abstract:

Contemporary hybrid threats simultaneously affect military systems, public administration, critical infrastructure, the information environment, and the public sense of security. They are characterised by a high level of uncertainty, ambiguity of warning signals, rapid situational change, and the deliberate exploitation of informational chaos. Under such conditions, defence education and crisis training cannot be limited to preparing specialised formations or mechanically reproducing procedures. Given the possibility of cascading effects and the inability to fully prepare for all types of threats, the development of social resilience becomes crucial. Social resilience is understood here as the capacity of society, institutions, and local communities to anticipate threats, absorb disruptions, adapt, maintain independent judgement, and restore essential functions during crises. The

aim of this study is to analyse the potential of immersive and simulation technologies in strengthening social resilience and independent thinking in the face of hybrid threats. Particular attention is devoted to the use of VR, AR, MR, CAVE environments, decision-making simulations, and scenario-based games in crisis management, civil defence, crisis communication, and countering disinformation. The research problem concerns how these technologies can support the transition from traditional defence education to an integrated resilience-oriented training model involving both military and civilian actors. Preliminary research findings make it possible to propose a framework model for the use of these technologies, taking into account ethical, organisational, cognitive, and data security-related risks. Particular emphasis is placed on information assessment, the recognition of manipulation, decision-making under incomplete information conditions, and the design of training programmes aimed at strengthening the adaptive capacity of societies and institutions during crises, as well as readiness for responsible practical action.

Keywords:

hybrid threats, social resilience, immersive technologies, independent thinking, defence education

2. **Tomáš Kolomazník**, **PhD** Metropolitan University Prague, Czech Republic, *Tools for combating disinformation in the public sphere in the age of artificial intelligence*

Abstract:

In the era of rapidly developing artificial intelligence (AI) technologies, state and government communication on social platforms in Central European countries faces a number of new challenges and constraints. One of the main challenges is undoubtedly the spread of AI-generated content. This phenomenon, commonly referred to as “Slopaganda”, involves the deliberate spread of low-quality AI-generated content with the aim of manipulating public perceptions and political processes with unprecedented speed and tailor-made precision. The aim of this paper is to analyse the current situation in Central European countries with an emphasis on the Czech Republic and Slovakia. The paper will present the current situation in these countries and the specific challenges they face. Disinformation campaigns generated by artificial intelligence pose significant challenges to combat them, as current mitigation strategies in the CEE region consistently demonstrate limited effectiveness. There are several reasons for this situation. These include undoubtedly low digital and media literacy of the population. The countries also suffer from a low level of development of the civil society. This analysis employs qualitative content analysis as its core method for systematically reviewing key policy texts. These include strategic documents on state communication, AI regulatory frameworks, and pertinent legal instruments. The approach identifies recurring patterns, themes, and discourses, promoting reproducible and objective insights. The analysis is further bolstered by semi-structured interviews with key stakeholders, such as strategic communication experts, drafters of national anti-disinformation strategies, and civil servants. These interviews enable critical scrutiny of official policies, highlighting implementation gaps and strategic alignments. Note: This paper is the result of Metropolitan University Prague research project no. E114-126 /2025 “Strategic communication of the state in the digital space: possibilities and limits of the state in communication on digital platforms” (2025 and 2026) funded by The Ministry of Education, Youth and Sports from the Funds for Support of Specific Research.

Keywords:

Strategic Communication, Artificial Intelligence, Slopaganda, Chatbots, Disinformation, Russia

3. **Krzysztof Zieliński**, **PhD** War Study University, Poland, *Social resilience and local crisis preparedness*

Abstract:

In the context of contemporary complex and cascading threats, social resilience has become a key resource for local crisis preparedness and an important dimension of public safety systems. This paper addresses the need to better conceptualize and operationalize social mechanisms that enhance the ability of local communities to cooperate, adapt, and recover from disruptions. The aim of the study is to organize these mechanisms by proposing an analytical framework based on a triad of trust, self-organization, and risk education. The paper is theoretical and conceptual in nature and is based on a critical analysis and synthesis of recent literature in the fields of social resilience, crisis management, and risk communication and education. The analysis demonstrates that the three components of the proposed framework are interdependent and mutually reinforcing. Trust stabilizes social cooperation and increases the legitimacy and acceptance of institutional actions. Self-organization enables the activation of local support networks and the mobilization of available resources. Risk education, in turn, develops the competencies necessary for informed decision-making and rational protective behaviour. The main conclusion is that effective local crisis preparedness requires the balanced and parallel development of all three components, as weakening any one of them reduces the overall sustainability of the system. The proposed triad may serve as a useful tool for diagnosis, comparative research, and the design of practical measures aimed at strengthening local resilience.

Keywords:

social resilience, crisis preparedness, trust, self-organization, risk education

4. **Wojciech Sługocki**, **PhD** Academy of Applied Sciences in Wrocław, Poland, *Rethinking Education in the New Infosphere: Systemic Responses to the Age of Disinformation*

Abstract:

The infosphere has undergone a profound transformation, yet education has failed to adapt at a comparable pace. Disinformation now functions as a strategic tool within hybrid influence operations, subtly normalising mistrust and weakening the bond between citizens and institutions. The central argument is straightforward: students should learn to identify disinformation the way medical professionals learn diagnosis through sustained engagement with real-world cases, in real time, with meaningful stakes. Abstract definitions of fake news do not build epistemic resilience. Direct exposure to genuine manipulation as it surfaces in everyday digital life does. The proposed response is a structural reorientation of curricula, integrating disinformation literacy across core subjects and educational stages rather than confining it to isolated modules. Drawing on research into generational competence gaps and the political psychology of institutional trust, the presentation argues that resilience to informational disorder is cultivated early, in the classroom. Democratic stability is not secured within institutions of governance alone. It is built, or quietly lost, in the habits of thought we succeed or fail in passing on.

Keywords:

infosphere, disinformation, media literacy, curricular reform, critical thinking

5. **Eng. Monika Zamłyńska**, Military University of Land Forces, *A model for cybersecurity competence development based on virtual environments and simulation driven learning*

Abstract:

The increasing complexity of cyber threats requires improved approaches to cybersecurity education, particularly in developing practical penetration testing skills. Traditional teaching methods are often insufficient to address current competency demands. This paper proposes a model for cybersecurity competence

development based on virtual environments and simulation-based learning. The approach leverages virtual laboratories, Capture The Flag (CTF) platforms, and virtual reality (VR) to create controlled and secure training conditions. These environments enable learners to simulate cyber attack scenarios, apply offensive techniques, and gain hands-on experience without affecting real systems. The proposed model emphasizes active learning and experiential training, supporting the development of analytical and decision-making skills. Simulation-based methods increase learner engagement and allow for repeatable, scalable training scenarios. The results indicate that integrating virtual and simulation-based environments into cybersecurity education enhances learning effectiveness and better prepares students for real-world security challenges.

Keywords:

cybersecurity, virtual environments, simulations, education, penetration testing, practical competencies

6. **prof. Katerina Veljanovska Blazhevska**, MIT University Skopje, North Macedonia, **prof. Dorota Domalewska,** War Studies University, Poland, **Piotr Okulski, MSc,** War Studies University, Poland, *Visual disinformation in social media: challenges and implications for education*

Abstract:

Social media environments are increasingly shaped by visual forms of communication, including images, videos, memes, and data visualisations. At the same time, visual content is becoming an important tool of disinformation, manipulation, and cognitive influence. Visual disinformation often affects emotions and perception more rapidly than textual messages, making it particularly challenging for users to critically assess the credibility and context of online content. The presentation discusses the growing role of visual disinformation in social media and its implications for education. Particular attention is devoted to the concept of visual literacy, understood as the ability to critically interpret, analyse, and evaluate visual information. The presentation highlights how visual manipulation techniques, including misleading images, edited videos, deepfakes, and decontextualised visuals, can influence public opinion, social attitudes, and decision-making processes. The discussion also addresses the need to strengthen educational approaches aimed at developing critical thinking and resistance to manipulation in digital environments. Emphasis is placed on the importance of teaching users how to recognise visual manipulation, assess the credibility of visual sources, and interpret visual data responsibly. The presentation argues that visual literacy should become an important element of contemporary media and security education in response to the challenges posed by social media and information warfare.

Keywords:

visual disinformation, social media, visual literacy, critical thinking, media education, cognitive warfare, manipulation, digital literacy

PANEL 4

Link: https://tinyurl.com/3f8sa429

Legal and Regulatory Challenges of Emerging Defence Technologies

1. **Karol Chaberka, MSc** University of Economics in Katowice, Poland, *From Visualization to Behavioural Change: Immersive Technologies as Instruments for Environmental ESG KPI Measurement and Governance in Defence and Security Contexts*

Abstract:

The environmental dimension of Environmental, Social, and Governance (ESG) frameworks constitutes a critical component of contemporary defence and security policies, particularly in the context of energy resilience, critical infrastructure protection, and sustainable operational readiness. Defence institutions and security-related organisations increasingly rely on environmental Key Performance Indicators (KPIs) to assess energy consumption, emissions, and resource efficiency; however, the complexity of such indicators often limits their effective interpretation and operational use by decision-makers and end-users. Role analysis of immersive technologies—Virtual Reality (VR) and Cave Automatic Virtual Environments (CAVE)—as enabling instruments for environmental ESG KPI interpretation, governance, and behaviour-oriented decision support within defence and security-related domains. Drawing on evidence from three complementary streams of prior research, the paper synthesises findings from urban sustainability planning, industrial training, and building energy performance. First, studies on VR-based visualization of environmental KPIs in zero-emission neighbourhoods demonstrate that immersive representation of lifecycle-based indicators, such as CO_2 emissions and energy demand, significantly improves stakeholder comprehension and supports coordinated decision-making—an aspect directly relevant to defence logistics hubs, military campuses, and critical infrastructure planning. Second, empirical results from industrial environments indicate that VR-supported training reduces material usage, limits the need for physical exercises, and shortens training cycles, thereby contributing to measurable environmental ESG outcomes while enhancing safety and operational efficiency. Third, recent CAVE-based interventions targeting energy-related behaviour reveal that immersive, feedback-driven environments can influence user decisions, leading to quantifiable reductions in energy consumption without compromising functional performance—an issue of growing importance for energy-intensive defence facilities. The paper argues that immersive environments should be understood not merely as educational or visualization tools, but as socio-technical instruments embedded in environmental governance systems. By enabling stakeholders to interact with environmental KPIs in realistic and controlled settings, VR and CAVE technologies support the transition from static ESG reporting toward dynamic, resilience-oriented governance models aligned with contemporary defence and security requirements.

Keywords:

Immersive Technologies, Environmental ESG Indicators, Defence and Security Governance, Energy Resilience and Sustainability, Decision-Making, Behavioural Change

2. **Eng Kacper Zdrojewski**, **MSc** War Studies University, Poland, *Preparing for Algorithmic Warfare: Immersive Learning, Human-in-the-Loop, and Regulatory Challenges*

Abstract:

The rapid integration of emerging technologies, specifically Artificial Intelligence (AI) and advanced simulation systems, into defence education is fundamentally transforming how military personnel prepare for modern armed conflicts. This presentation explores the expanding role of simulation-based learning and immersive environments as essential pedagogical tools in both military and civilian training. By creating dynamic and complex crisis scenarios, these tools offer unprecedented opportunities to develop strategic decision-making skills and enhance institutional resilience. However, deploying algorithmic systems in military contexts extends beyond tactical simulation. It necessitates rigorous training in governance and ethical oversight. This presentation emphasizes the critical importance of embedding the "Human-in-the-Loop" (HITL) concept within training curricula. As autonomous and semi-autonomous systems become more prevalent on the battlefield, educational frameworks must be designed not only to teach warfighting but also to train operators in maintaining meaningful human control over AI-driven processes. Furthermore, the discussion addresses the complex regulatory environment surrounding military AI. It examines how current international legal frameworks and

their existing gaps must be incorporated into simulation scenarios. This practical integration is crucial to adequately prepare future commanders for the legal ambiguities of algorithmic warfare. By bridging simulation technologies with critical governance and regulatory perspectives, this session highlights how modern defence education must evolve. Technology-enhanced training is vital not only for tactical proficiency but also for instilling the ethical and legal principles required for the responsible adoption of new technologies in global security contexts.

Keywords:

Simulation-Based Learning, Immersive Technologies, Artificial Intelligence, Defence Education, AI Regulation

3. **Ignacy Klajbor**, University of Gdańsk, Poland, *Legal Frameworks and Regulatory Challenges in the Implementation of Artificial Intelligence in Immersive Defence Training Systems*

Abstract:

The integration of artificial intelligence (AI) with immersive technologies (VR, AR, MR) is transforming defence training systems and enhancing preparedness for crisis response. However, the rapid pace of technological development increasingly outstrips existing legal frameworks, creating regulatory gaps related to national security and the protection of sensitive data, including biometric information. This study aims to identify and analyse key legal and regulatory challenges associated with the implementation of AI-driven solutions in defence training environments. Particular attention is given to issues of liability, accountability, and algorithmic transparency. The research is based on a doctrinal legal method, involving a systematic analysis and interpretation of relevant legal acts. The study examines recent European Union regulations, including the AI Act, as well as national provisions related to defence and cybersecurity. The legal analysis is complemented by a review of technical reports and industry publications to contextualise the findings within current technological developments. The results indicate significant deficiencies in existing regulatory approaches, particularly in relation to responsibility for system errors and the lack of clear certification standards for AI-supported training systems. These gaps may limit the safe and effective deployment of such technologies. The study concludes that the successful integration of AI in defence education requires not only technological advancement but also coherent and adaptive legal frameworks.

Keywords:

Artificial Intelligence; Virtual Reality; Immersive Technologies; Defence Training; Legal Frameworks; AI Regulation; Algorithmic Transparency

4. **Jan Szych**, University of Warsaw, Poland, *Fiscal engineering as a governance tool in technology-driven security systems: balancing efficiency and fundamental rights*

Abstract:

The rapid integration of dual-use technologies, such as immersive VR/AR systems, autonomous devices, and data-driven infrastructures, defence education and broader security governance challenges traditional regulatory paradigms. This presentation advances an alternative approach grounded in fiscal engineering, understood as the strategic use of indirect taxation and regulatory levies to shape technological deployment in security-sensitive contexts. Departing from the increasingly problematic taxation of intangible digital services, the analysis draws on the classical doctrine of public finance, in particular the subjective theory of excisable goods. Within this framework, taxation is linked to the intended use (przeznaczenie) of a tangible object. As a result, technologically neutral hardware may be subject to differentiated fiscal regimes depending on whether it is used for defence training and crisis preparedness, or for civilian purposes that generate negative externalities. This

approach allows the state to indirectly govern security ecosystems through legally structured economic incentives, without overextending traditional regulatory tools. The presentation also examines the shift toward compliance-by-design models, where real-time, centralized data systems automate fiscal oversight. While these architectures enhance efficiency and state resilience, they simultaneously risk creating quasi-surveillance environments. Applying the principle of proportionality - suitability, necessity, and proportionality stricto sensu the study highlights the growing tension between technological governance and the protection of fundamental rights. It is argued that redefining taxable events around the functional purpose of physical technologies offers a doctrinally coherent and operationally viable framework for regulating emerging security systems in democratic societies.

Keywords:

fiscal engineering, dual-use technologies, security governance, defence education, indirect taxation, excise taxation, compliance by design, data-driven regulation, proportionality principle, technology governance

5. **Anna Stawińska**, Cardinal Stefan Wyszyński University, Poland, *Legal and Economic Determinants of Implementing Immersive Technologies in Defence Training Systems - Institutional and Market Perspective*

Abstract:

The rapid development of immersive technologies - including Virtual Reality (VR), Augmented Reality (AR), Mixed Reality (MR), and CAVE environments - creates new opportunities for defence training systems while simultaneously generating complex challenges of a legal, economic, and managerial nature. This paper undertakes a comprehensive analysis of the institutional and market conditions for deploying these technologies in the defence and security sector. The analysis encompasses three interrelated dimensions: the legal perspective, including applicable EU regulatory frameworks (the AI Act, cybersecurity directives, and public procurement law in the defence sector); the economic perspective, covering cost-benefit analysis, dual-use technology financing models, and impacts on the defence industry market structure; and the institutional dimension, focusing on the organisational readiness of military and civilian institutions to absorb new training technologies. The paper draws on case studies of VR/AR system deployments in selected NATO countries, with particular emphasis on Polish experiences, and a review of current international and national regulations. The findings indicate a significant regulatory gap between the pace of technological development and the adaptive capacity of the legal system, as well as the need for dedicated financing models for small and medium-sized enterprises in the defence sector. The research conclusions point to the need for an integrated approach combining legal regulations, financial instruments, and organisational change management strategies as a prerequisite for the effective and responsible deployment of immersive technologies in defence education and training.

Keywords:

immersive technologies, defence training, legal regulations, AI Act, defence economics, dual-use, VR/AR, defence procurement, institutional governance

6. **Andrzej Kozik**, University of Gdańsk, Poland, *Regulating the Smart Threat: Legal and Governance Challenges in Restricting Foreign Connected Devices in the Context of National Security*

Abstract:

The rapid integration of emerging technologies, particularly connected devices, into national defense infrastructures introduces unprecedented vulnerabilities. As foreign-manufactured smart devices become ubiquitous, they present significant intelligence and operational risks. Consequently, establishing robust regulatory environments is crucial to mitigate these threats and ensure national safety. This study aims to analyze

the legal and governance challenges associated with restricting foreign connected devices within the defense and security sector. It seeks to identify gaps in current institutional frameworks and propose actionable regulatory strategies to enhance sector resilience. The research was undertaken through a comprehensive legal and policy analysis of existing national and international regulatory frameworks. This included comparative case studies of recent legislative efforts aimed at mitigating technological espionage and supply chain vulnerabilities in defence contexts. The findings indicate that current regulatory environments often lag behind rapid technological advancements, creating critical vulnerabilities. Governance structures struggle with inter-organisational coordination, and restrictive measures frequently clash with international trade laws and the practical necessity of utilizing commercial off-the-shelf (COTS) technologies. These results underscore a fundamental tension between maintaining a technological advantage through global supply chains and ensuring absolute operational security. The evaluation reveals that reactive, fragmented legislation is highly insufficient to counter the persistent and evolving "smart threat." In conclusion, safeguarding national safety requires a paradigm shift from reactive device banning to proactive, resilience-based technology governance. Developing adaptive legal frameworks and standardized risk-assessment protocols is vital to securely integrate emerging technologies while effectively mitigating foreign intelligence threats.

Keywords:

Critical Infrastructure, Cyber Defense, Intelligence Risks, National security, Technological Espionage

PANEL 5

Link: https://tinyurl.com/3y74t85m

Hybrid Threats, Strategic Governance and Critical Infrastructure Security

1. **prof. Weronika Jakubczak**, Fire University, Poland, *Cyber Education for Security in the IoT and IoE Ecosystem: Immersive Technologies for Building Cyber Resilience in Hybrid Conflicts*

Abstract:

Contemporary cybersecurity education must respond to an environment in which the boundaries between humans, devices, networks, and organisations are becoming increasingly blurred. The development of the Internet of Things (IoT) and the Internet of Everything (IoE) means that the object of protection is no longer limited to information systems alone, but also includes social processes, critical infrastructure, public services, households, and the everyday behaviour of users. Under such conditions, cybersecurity requires not only technical competencies but also cyber resilience, understood as the ability of individuals, institutions, and communities to anticipate threats, mitigate the effects of incidents, adapt, and rapidly restore functions after disruption. The aim of this study is to analyse the role of cybersecurity education in shaping security within the IoT and IoE ecosystem, with particular emphasis on immersive technologies. VR, AR, MR, CAVE environments, cyberattack simulations, and scenario-based games can support experiential learning, develop situational awareness, critical thinking, digital hygiene, and incident response capabilities. The research problem concerns how immersive technologies can transform traditional cybersecurity education into an integrated resilience-oriented training model. Preliminary findings make it possible to identify a framework model of cybersecurity education encompassing cognitive, technological, behavioural, and organisational dimensions. Particular emphasis is placed on risks related to dependence on connected devices, data protection, disinformation, user errors, and the need to build a culture of cyber resilience in the context of hybrid threats and cognitive warfare.

Keywords:

cybersecurity education, cybersecurity, Internet of Things (IoT), Internet of Everything (IoE), cyber resilience, immersive technologies

2. **CDR Krzysztof Pająk**, **PhD** War Study University, Poland War Study University, Poland, *'No Boots on the Ground': Challenges and Implications of Removing Human Presence from Military Doctrine and Operations*

Abstract:

This article examines the challenges and implications of removing human presence from military doctrine and operations by assessing the feasibility of a "No Boots on the Ground" approach. It explores how such a shift would affect the strategic culture of armed forces and the political level of the state, particularly in terms of decision-making thresholds for the use of force, public accountability, and democratic oversight. By reducing risks to soldiers, this approach may lower the domestic political costs of military engagement, potentially enabling more frequent or less publicly contested deployments. At the same time, it raises critical questions about legitimacy, responsibility for the use of autonomous systems, and the transparency of military actions, thereby reshaping civil-military relations and the ways governments justify operations to domestic and international audiences. Particular attention is given to technological advancements enabling autonomous and remotely conducted operations and their impact on operational planning, force structure, and doctrinal development. The growing reliance on artificial intelligence, unmanned systems, and network-centric capabilities challenges traditional principles of warfare, including mass, maneuver, and human-centered command. The article also identifies key obstacles to implementing a "No Boots on the Ground" policy, such as institutional resistance, technological limitations, and vulnerabilities to cyber and electronic warfare. These challenges are further complicated by concerns regarding accountability, rules of engagement, and compliance with international law. Overall, the study offers a balanced assessment of whether removing human presence from the battlefield is a feasible and sustainable direction for future military operations.

Keywords:

autonomous operations, future operational environment, future combat, human presence in military operations and doctrines

3. **Lieut. Cmdr. George Margaros**, Hellenic Navy, *Quantitative Decision Study on the Integration of Nuclear Energy into a Country*

Abstract:

This study examines the role of nuclear energy in enhancing national energy security under conditions of uncertainty and complex decision-making. As global energy demand rises, driven by technological advancements and geopolitical instability traditional energy strategies are increasingly insufficient. The research focuses on Greece as a representative case, given its high energy dependence and recent economic challenges, while proposing a methodological framework applicable to other countries. A fuzzy logic model is developed to evaluate energy security based on the level of nuclear energy penetration. Integrating key variables, including energy dependence, diversification, efficiency, renewable energy penetration, geopolitical risk, and nuclear development. This approach allows for the quantification of qualitative and uncertain parameters through linguistic variables (e.g., low, medium, high) and rule-based inference. Mathematical functions describe the dynamic relationships between nuclear energy penetration and each indicator. The results indicate that nuclear energy can significantly improve energy security, particularly by reducing import dependence and enhancing system stability. A critical threshold is identified at approximately 30–40% nuclear penetration, where the most substantial gains in energy security occur. Beyond this range, improvements diminish, especially under

conditions of elevated geopolitical tension, which constrains the overall effectiveness of nuclear expansion. The study concludes that nuclear energy, particularly through Small Modular Reactors, can serve as a strategic component of a diversified energy mix. However, its success depends on broader factors, including geopolitical conditions, public acceptance, and complementary investments in renewable energy and infrastructure.

Keywords:

Nuclear Energy, Fuzzy Logic, Small Modular Reactors, Geopolitical Risk

4. **Achille Castrogiovanni**, **PhD** University of Sunderland, United Kingdom, *Hybrid Coercion and Maritime Deterrence in the Baltic Sea: Critical Undersea Infrastructure and Narrative Contestation*

Abstract:

This paper examines maritime hybrid coercion in the Baltic Sea through the interaction of critical undersea infrastructure vulnerability, shadow-fleet activity, deterrence adaptation, and competing official narratives. It asks how recent NATO, EU, and regionally oriented policy documents, when read alongside selected Russian official statements and doctrines, conceptualise the Baltic maritime security challenge and what this reveals about deterrence and escalation in a contested maritime theatre. Methodologically, the paper employs qualitative comparative document analysis and structured close reading of three source clusters: analytical assessments, Western official policy outputs, and Russian official narratives. The analysis is organised around four indicators: coercive mechanisms, deterrence mechanisms, escalation dynamics, and narrative framing. The paper argues that maritime hybrid coercion in the Baltic operates through the interaction of material disruption, legal and attributional ambiguity, and contestation over legitimacy, blame, and escalation. It finds that effective deterrence in this setting cannot rest on naval capability alone. Rather, it depends on the integration of infrastructure resilience, surveillance, regulatory and legal adaptation, improved attribution, and credible strategic communication. The Baltic case therefore demonstrates that infrastructure protection, narrative contestation, and conventional readiness are mutually constitutive elements of maritime deterrence. At the same time, the paper advances a bounded claim: it does not treat every incident as proof of a seamless Russian campaign or as evidence of imminent large-scale war, but shows how repeated below-threshold activity can nonetheless compress decision time, complicate response, and shape escalation risk in a strategically significant region.

Keywords:

Hybrid Coercion, Maritime Deterrence, Baltic, Critical Infrastructure

5. **Jari Hautamäki**, Jyväskylä University of Applied Sciences, *Cybersecurity Intelligence Sharing Model*

Abstract:

Cybersecurity has become an essential element of societal resilience as digitalisation has increased the dependence of authorities, organisations, and citizens on information systems, networks, and digital services. At the same time, cyber threats have grown both in volume and complexity. Attacks frequently target multiple organisations simultaneously, with threat actors reusing similar tactics, techniques, and vulnerabilities across different contexts. However, individual organisations typically observe threats from a limited, organisation-specific perspective, making it difficult to form a comprehensive situational picture. Consequently, cyber threat intelligence sharing has emerged as a key mechanism for improving collective defense and situational awareness. This study is based on the premise that threat intelligence sharing is not solely a technical challenge, but also an organisational, social, and strategic phenomenon. Effective sharing requires trust between participating actors, shared rules and practices, and suitable structures for representing and exchanging threat

information. The research was conducted using a constructive research approach and comprises several interconnected sub-studies in which a cyber threat intelligence sharing model was developed iteratively. The initial phase focused on theoretical network modelling and simulation, while later phases involved practical evaluation in national cybersecurity exercises. These exercises provided a realistic environment for assessing intelligence sharing under conditions of time pressure and high decision-making demands. The results demonstrate that threat intelligence sharing was perceived as highly valuable. Most participants actively utilised information shared by others, particularly for threat analysis and situational awareness. However, despite the perceived usefulness of structured sharing platforms, their adoption was not yet fully established, and a significant amount of threat intelligence continued to be exchanged through informal communication channels such as email and telephone.

Keywords:

Cyber Security, Situational Awareness, Cyber Threat Intelligence Sharing

6. **Pedro Silva Baptista**, Minho University, Portugal, *Epistemic Sovereignty in the Battlespace: Human Capital and the Governance of Emerging Defense Technologies in African States*

Abstract:

As new and emerging technologies fundamentally alter the landscape of global security, African defense sectors face a critical inflection point. This paper argues that the mere acquisition of advanced military hardware or simulation technologies does not equate to sovereign defense capability. Instead, it frequently exacerbates the paradigm of "States in Africa"—where nations act as passive vessels for foreign military technologies and external geopolitical competition. To transition into sovereign "African States" capable of endogenous defense statecraft, military institutions must achieve epistemic sovereignty. Grounded in an analysis of human capital and defense education, this paper demonstrates that technological resilience in the defense sector is fundamentally constrained by a broader crisis in educational alignment and "learning poverty." Without highly skilled officer corps and robust professional military education (PME) frameworks, states lack the capacity to govern, regulate, and effectively integrate emerging technologies into their operational domains. By focusing on governance-related challenges and institutional resilience, this paper proposes that the strategic modernization of defense education and training in Africa is not merely an administrative upgrade, but the primary geostrategic mechanism for securing true operational autonomy and geopolitical agency in the 21st-century battlespace.

Keywords:

emerging technologies, defence education, Professional Military Education (PME), epistemic sovereignty, African security, military modernisation, institutional resilience, operational autonomy, human capital, geopolitical agency

7. **Joanna Pastuszak-Cybulska,** MsC University of the National Education Commission in Krakow *From exclusion to inclusion: addressing the challenges of alerting deaf people to danger*

Abstract:

This presentation examines the persistent exclusion of deaf people from mainstream emergency warning practices and proposes pathways towards genuinely inclusive alerting systems. Drawing on insights from disability studies, risk communication, and human–computer interaction, it frames current emergency infrastructures as implicitly audio-centric, systematically privileging hearing users. As a result, many deaf individuals receive delayed, incomplete, or no information at all about imminent threats such as fires, natural

disasters, or security incidents. The talk identifies key challenges at three levels: technological (limited multimodal interfaces, poor integration of visual and tactile alerts, lack of interoperability), organizational (fragmented responsibilities, inconsistent standards, and unequal availability of accessible solutions), and socio-cultural (as an limited involvement of deaf communities in design and policy processes). Ultimately, the talk argues that moving from exclusion to inclusion in danger communication requires not only new devices, but a systemic reimagining of what a "universal" warning system should be. In the end, an example of assistance dogs wil be shown as a valuable component of the system for warning the deaf against danger.

Keywords:

deafness, national security, deaf alert systems

Conference Closing:

14:30 – 15:00

Link: https://tinyurl.com/3f8sa429

Keynote speaker:

prof. Bert Chapman, Purdue University, United States, *Artificial Intelligence in the Curriculum of U.S. Professional Military Educational Institutions*

Abstract:

This presentation examines the growing integration of artificial intelligence into Professional Military Education (PME) at major undergraduate U.S. service academies, including the U.S. Air Force Academy, the U.S. Military Academy, and the U.S. Naval Academy. It discusses how AI-related education increasingly extends beyond computer science and engineering into fields such as military strategy, law, ethics, political science, and decision-making. Particular attention is devoted to interdisciplinary approaches combining technical competencies with ethical reflection, critical thinking, and operational decision-making under uncertainty. The presentation also addresses the role of libraries, research centres, and simulation-based learning environments in supporting AI education and research. The discussion highlights both the opportunities and challenges associated with the growing role of AI in military education, including ethical concerns, the limits of automation in warfare, and the continuing importance of human judgement in military decision-making.

Keywords:

artificial intelligence, Professional Military Education (PME), military education, U.S. service academies, military decision-making, ethics of AI, interdisciplinary education, simulation-based learning


SECURITY
&
DEFENCE
QUARTERLY


POLITECHNIKA
GDAŃSKA


WYDZIAŁ ELEKTRONIKI,
TELEKOMUNIKACJI
I INFORMATYKI


ARGON
World Leaders in CBRN/
HazMat training systems


SZKOŁA
DOKTORSKA
Akademii Sztuki Wojennej


МИТ УНИВЕРЗИТЕТ


POLITECHNIKA
RZESZOWSKA
im. IGNACEGO ŁUKASIEWICZA
Integra AV
Audio Video & Virtual Reality


megmar