INTERNATIONAL CONFRERENCE

AI FRONTIERS IN CYBERSECURITY AND INFRASTRUCTURE PROTECTION

Security and Defence Quarterly and the Doctoral School of War Studies University, Poland, are pleased to announce the International Conference on AI Frontiers in Cybersecurity and Infrastructure Protection.

22 May 2025

PROGRAMME

09:00 – 10:00 **(Central European Standard Time - Poland)**

Conference opening
Link: https://tinyurl.com/5n7puk5m
Col. prof. Andrzej Soboń, Dean of National Security Faculty, War Studies University, Poland

Keynote:

prof. Tegg Westbrook, University of Stavanger, Norway, *Will "off the shelf" artificial intelligence make complex-coordinated RFI tactics and strategies easier and more destructive?*

prof. Jacek Lebiedź, Gdańsk University of Technology, Poland, *Virtual Reality in security training: Case study based on the immersive 3D visualization lab*

10:00 – 12:00

Panel 1: AI for Infrastructure, Transport & Crisis Management
Link: https://tinyurl.com/5n7puk5m

Panel 2: AI in Law, Ethics, and Governance
Link: https://tinyurl.com/2sx9ysjb
Chair: **dr Przemysław Gasztold**, War Studies University

Chair: prof. Panagiotis Palaios, the American College of Greece, **dr Joanna Przybylak,** War Studies University

dr Andrzej Jarynowski, Freie Universität Berlin & Polish Hygienic Society in Wrocław – *Using AI-Enabled Real-Time Media Monitoring to Assess Animal Welfare During Crises: Insights from the Iberian Blackout (April 2025) and Central European Flood (2024)*

dr inż. Maciej Grunt, Pomeranian University in Słupsk – *AI in the Digital Transformation of Technical Protection Systems: New Approaches to Predictive Security Analytics*

mgr inż. Sonia Rozbiewska, *Maritime University in Szczecin – The Use of Artificial Intelligence in Forecasting and Mitigating the Risk of Pirate Attacks on Maritime Routes*

mgr Arkadiusz Olejarz, War Studies University – *The Impact of Artificial Intelligence on the Safety and Security of Cabin Crew in Civil Aviation*

Kamil Jan Margielewicz, *University of Silesia – Potential Application of Artificial Intelligence in Defense Systems Aimed at Protecting Critical Infrastructure: Context of EU Member States*

Vladyslav Budnyk, *University of Warmia and Mazury in Olsztyn (Ełk Branch) – AI-Driven Threat Detection: Balancing Security and Privacy in Critical Infrastructure Protection*

dr hab. Danuta Kaźmierczak, University of The National Education Commission – *AI – a Student's Ally or Distractor?*

dr Inna Kulish, State institution Institute of Regional Researchnamed after M.I. Dolishniy of the NAS of Ukraine**, Yana Mazur**, Lviv Polytechnic National University – *Artificial Intelligence and the Public Interest: Between Technology Autonomy and Human Responsibility*

mgr Anna Kremplewska, War Studies University – *Implementation of Artificial Intelligence in the Justice System: Opportunities for Development and Risks to Stability of the Judicial and Cyber Security*

mgr Jadwiga Stryczyńska-Najmowicz, WKB Lawyers – *Regulating the Digital Soldier: Legal Frameworks for AI in Military Operations*

mgr Maciej Czyszczoń, University of The National Education Commission in Krakow – *Artificial Intelligence as a Moral Agent? Challenges and Implications of James Moor's Classification*

mgr Dawid Trela, War Studies University – *Artificial Intelligence in Financial Security: Legal Challenges in Japan's AML/CFT Regime and Comparative Insights from Selected EU Countries*

Klaudia Banasiewicz, Lodz University of Technology – *AI in Cybersecurity: Innovations, Challenges, and Future Trends*

12:00 – 14:30

Panel 3: AI in Military and Defence Applications
Link: https://tinyurl.com/5n7puk5m
Chair: **dr hab. Dorota Domalewska**, War Studies University

prof. Anastasios-Nikolaos Kanellopoulos, Athens University of Economics and Business – *Integrating AI into Counterintelligence: A New Security Paradigm*

inż. Paweł Jaskuła, **inż. Maria Kamińska,** Lublin University of Technology – *Utilizing AI for Military Operational Planning and Simulation*

Lt. PhD Iwona Szkudlarek, University of Warsaw – *Professional Development of Soldiers: Immersive Technologies in Teaching Military English*

dr Krzysztof Pająk, War Studies University – *Enhancing Maritime Infrastructure Security through AI-Driven Naval Drone Operations in the Southern Baltic*

PhD Candidate Sunny Anand, University of Allahabad **–** *Role of AI in Modern War*

mgr Patryk Niksa, War Studies University – *Military Applications of Artificial Intelligence*

Kamil Jan Margielewicz, University of Silesia in Katowice &

Panel 4: AI for Cybersecurity: Defending Critical Systems and Infrastructure
Link: https://tinyurl.com/2sx9ysjb
Chair: dr hab. Małgorzata Gawlik Kobylińska, War Studies University

dr Pedro Silva Baptista, University of Minho – *AI-Driven Cybersecurity: Balancing Innovation, Security, and Ethical Challenges in Critical Infrastructure Protection*

prof. George Zombanakis, prof. Vasileios Symeonidis, The American College of Greece – *Defending Defence: The Demand for Cybersecurity Expenditures by the Hellenic MOD*

Cmdr. Amila Prasanga, Sri Lanka Navy, Leveraging AI for Subsea Cable Protection: Maritime Security Imperatives for Sri Lanka and Vulnerable Island States

dr Karol Chlasta, Kozminski University (WarsawIQ) – *Generative AI in Cybersecurity: Emerging Threats, Defensive Strategies, and Standards*

mgr Marceli Hązła, Poznan University of Economics and Business – *Quantum Technology as a Determinant of Cybersecurity and Technological Sovereignty of the European Union*

Wiktor Wilkołaski, War Studies University – *Towards Quantum-Resilient Systems: Introducing the AI-Enhanced Cryptographic Agility*

Upper Silesian University – *Selected Automatic Weapon Systems of NATO Member States: Context of AI Application*

Framework (AI-ECAF) Empowered by Post-Quantum Cryptography

Islam Hajiyev, Maria Curie-Skłodowska University – *The Role of Quantum Technologies in Future Cybersecurity Strategies*

14:30 – 15:00 **Conference Closing**

keynote speech

prof. Bert Chapman, Purdue University, USA, *Selected Artificial Intelligence Provisions in U.S. Fiscal Year 2025 National Defense Authorization Act*

Link: https://tinyurl.com/5n7puk5m

BOOK OF ABSTRACTS

Keynote:

Col. prof. Andrzej Soboń, Dean of National Security Faculty, War Studies University, Poland

prof. Tegg Westbrook, University of Stavanger, Norway, *Will "off the shelf" artificial intelligence make complex-coordinated RFI tactics and strategies easier and more destructive?*

prof. Jacek Lebiedź, Gdańsk University of Technology, Poland, *Virtual Reality in security training: Case study based on the immersive 3D visualization lab*

Link: https://tinyurl.com/5n7puk5m

Panel 1: AI for Infrastructure, Transport & Crisis Management
10:00 – 12:00
Link: https://tinyurl.com/5n7puk5m

Author	Title	Abstract
dr Andrzej Jarynowski	*Using AI-Enabled Real-Time Media Monitoring to Assess Animal Welfare During Crises: Insights from the Iberian Blackout (April 2025) and Central European Flood (2024)*	On April 28, 2025, an unprecedented power outage struck nearly the entire Iberian Peninsula and on a separate occasion in 2024, Central Europe experienced devastating floods that disrupted communities and critical infrastructure. In both events, state-of-the-art artificial intelligence systems facilitated real-time media monitoring, enabling rapid assessment of animal welfare impacts and the evolution of public discourse during these crises. During the blackout, AI-driven analysis captured a diverse array of issues: from the immediate challenges encountered on dairy farms—where the failure of milking robots and milk-cooling systems led to the spoilage of approximately 24 million liters of milk—to the temporary stress observed in household pets, as well as public responses to large-scale animal welfare emergencies. Similarly, during the 2024 flood crisis in Central Europe, the same monitoring framework revealed significant communication gaps in crisis messaging. Detailed discourse analysis highlighted how fragmented, emotionally charged narratives and the lack of targeted crisis communication for animal owners exacerbated the public's anxiety and hampered effective coordination among emergency services. In both contexts, the AI-enabled platform not only detected sentiment peaks—such as an early boost in positive public sentiment during the restoration phase of the blackout—but also provided critical insights into structural vulnerabilities within animal agriculture and companion animal management. The comparative findings underscore the growing reliance of modern society on uninterrupted emergency communication systems with the society, while emphasizing that effective crisis management must incorporate interdisciplinary approaches. Such strategies should integrate advanced data analytics for monitoring, targeted messaging tailored for diverse stakeholder groups. These lessons suggest that the integration of AI-driven monitoring with a nuanced understanding of crisis discourse can significantly enhance preparedness and response efforts in safeguarding animal welfare during wide-scale emergencies.
dr inż. Maciej Grunt	*AI in the Digital Transformation of Technical Protection Systems: New Approaches to Predictive Security Analytics*	AI in the Digital Transformation of Technical Protection Systems: New Approaches to Predictive Security Analytics ## Abstract This paper examines the integration of artificial intelligence in technical protection systems for critical infrastructure security. The research addresses the growing challenge of cyber threats and the limitations of traditional security systems through predictive modeling based on legacy system data. Our SAFEGUARD framework (Secure Adaptation Framework for Enhancing Governance and Utilization of AI in

		Resilient Domains) offers a comprehensive methodology for implementing AI-driven security solutions in critical infrastructure environments. We present findings from a pilot project conducted across critical infrastructure locations in Poland, which collected data from multiple heterogeneous technical systems. The study demonstrates the efficacy of combining various machine learning algorithms with integrated data from access control systems, HVAC, power supply, and other technical protection sources to create effective predictive models. Results show significant improvements in risk detection, response times, and system availability. The paper concludes with strategic recommendations for organizations seeking to enhance security posture through AI integration, addressing technical, organizational, and ethical challenges in implementation. This research contributes to the development of more resilient critical infrastructure protection through proactive security management.
mgr inż. Sonia Rozbiewska	*The Use of Artificial Intelligence in Forecasting and Mitigating the Risk of Pirate Attacks on Maritime Routes*	Maritime piracy remains a significant challenge for international security and global trade, threatening the stability of key shipping routes and imposing considerable economic and operational risks on the maritime industry. Traditional methods of risk management, while effective in the past, are increasingly insufficient to address the dynamic and evolving nature of piracy threats. In this context, artificial intelligence (AI) provides innovative tools for analyzing, forecasting, and mitigating risks associated with pirate attacks. This presentation explores the application of AI in managing the risk of maritime piracy, focusing on predictive models and real-time threat analysis. Using a dataset of documented pirate attacks, key risk factors such as geographic locations, timeframes, vessel types, and environmental conditions are analyzed to uncover patterns and trends. Machine learning algorithms are then employed to predict high-risk areas, enabling proactive measures to safeguard vessels and crews. Additionally, the integration of AI with real-time monitoring systems offers dynamic risk management, facilitating quick decision-making and adaptive security measures. The benefits of AI-driven solutions in this domain include enhanced accuracy in threat detection, reduced costs associated with security operations, and increased efficiency of preventive actions. By combining advanced technology with traditional maritime security practices, this approach offers a comprehensive strategy to combat piracy in the 21st century. The findings emphasize that leveraging AI in risk management has the potential to revolutionize maritime security and ensure the protection of global trade routes in an ever-changing risk environment.
mgr Arkadiusz Olejarz	*The Impact of Artificial*	Artificial intelligence is becoming more and more common in civil aviation. The aim of this

	Intelligence on the Safety and Security of Cabin Crew in Civil Aviation	article is to present how artificial intelligence affects the level of safety and security of cabin crew in civil aviation and how cabin crew approach to artificial intelligence has changed.
Kamil Jan Margielewicz	*Potential Application of Artificial Intelligence in Defense Systems Aimed at Protecting Critical Infrastructure: Context of EU Member States*	During my speech, I would like to present the broadly understood possibilities of using artificial intelligence in systems aimed at protecting critical infrastructure. I am inclined to such a topic due to my own interest in the subject, the desire to show potential new applications of artificial intelligence in accordance with the understanding of defense, and also due to the current geopolitical situation in the world, and the ongoing technological development. I would present specific examples of the above-mentioned applications of artificial intelligence in accordance with the understanding of defense in the realities of the 21st century. In general, my entire presentation will concern the topic of the possibilities of using artificial intelligence in the context of defense, taking into account the examples of the European Union member states. In a few final sentences, I would also mention the positive and negative aspects of using artificial intelligence in its application, concerning defense. The topic was developed on the basis of library and archive research, the author's experience and knowledge in the thematic scope of the paper, as well as on the basis of selected statements of experts and experts on the subject, which have been made public.
Vladyslav Budnyk	*AI-Driven Threat Detection: Balancing Security and Privacy in Critical Infrastructure Protection*	As artificial intelligence (AI) continues to transform cybersecurity, its role in protecting critical infrastructure has become increasingly vital. AI-powered threat detection systems offer unparalleled capabilities in identifying and mitigating cyber threats in real time. However, their deployment raises significant concerns regarding data privacy, ethical considerations, and potential biases in decision-making. This paper explores the challenges and opportunities of AI-driven threat detection, focusing on balancing security imperatives with privacy protections. It examines existing regulatory frameworks, best practices, and future directions for ensuring AI-driven cybersecurity solutions remain both effective and ethically sound. The discussion also highlights the need for transparent AI models, responsible data handling, and interdisciplinary collaboration to strengthen infrastructure resilience against emerging cyber threats.
Panel II: AI in Law, Ethics, and Governance **10:00 – 12:00** **Link:** https://tinyurl.com/2sx9ysjb		

dr hab. Danuta Kaźmierczak	*AI – a Student's Ally or Distractor?*	The presentatation will discuss the findings of the empircal research on the AI application in the teaching environment from the users' perspective.
dr Inna Kulish, Yana Mazur	*Artificial Intelligence and the Public Interest: Between Technology Autonomy and Human Responsibility*	The paper examines the challenges of regulating artificial intelligence (AI) in a way that serves the public interest, particularly focusing on the tension between the autonomy of intelligent systems and human responsibility. The authors argue that current legal and ethical frameworks often lag behind technological developments, creating uncertainty in assigning accountability for the consequences of AI decisions. Emphasis is placed on the importance of maintaining human oversight and the principles of democratic control over automated decision-making processes. The paper explores the limitations of algorithmic transparency, the risks of over-reliance on machine autonomy, and the need for cross-sectoral collaboration in shaping effective regulatory approaches. Special attention is given to the role of public administration in ensuring that AI technologies are used in a manner consistent with the rule of law, human rights, and social justice. The authors propose directions for strengthening institutional mechanisms of responsibility and suggest principles for AI regulation that reflect the values of democratic governance. The paper highlights the importance of adaptive and forward-looking regulation that can respond to rapid technological changes without compromising core societal values. Ultimately, it contributes to the broader discourse on ethical innovation and the role of government in guiding technological development in line with public accountability.
mgr Anna Kremplewska	*Implementation of Artificial Intelligence in the Justice System: Opportunities for Development and Risks to Stability of the Judicial and Cyber Security*	The article examines the implementation of modern technologies and artificial intelligence within the Polish judiciary, highlighting both the opportunities they present and the potential risks to legal and cyber security. The paper identifies a range of opportunities for the judiciary, including the automation of case identification and legal analysis through artificial intelligence, enhanced access to justice for citizens, and improved consistency and predictability in judicial decision-making. The article also explores the challenges courts face, such as practical issues related to the deepfakes and the creation of falsified documents by generative artificial intelligence, along with their potential impact on evidence and judicial proceedings. The risks related to algorithmic errors and possible infringements of the principle of judicial independence are also highlighted. Furthermore, the issue of algorithmic bias is considered, particularly its implications for the rights of parties to proceedings and the right to a fair trial. The article further explores the influence of artificial intelligence on court operations, illustrating how AI may support judicial proceedings. It references existing and planned pilot projects involving AI

		within the judiciary. Moreover, the article addresses risks to the cybersecurity of judicial systems and legal risks related to the deployment of artificial intelligence, with particular attention given to safeguarding the integrity of court infrastructure and the protection of sensitive data processed within court registers and systems.
mgr Jadwiga Stryczyńska-Najmowicz	*Regulating the Digital Soldier: Legal Frameworks for AI in Military Operations*	As artificial intelligence (AI) becomes increasingly integrated into modern military systems, the legal and ethical implications of its deployment on the battlefield demand urgent and rigorous analysis. The emergence of autonomous and semi-autonomous technologies—ranging from decision-support systems to lethal autonomous weapon systems (LAWS)—is transforming not only the nature of warfare but also the responsibilities of states, commanders, and developers. This presentation explores the current legal frameworks governing the use of AI in military operations, focusing on international humanitarian law (IHL), international human rights law (IHRL), and state responsibility. Particular attention is paid to the principles of distinction, proportionality, and accountability, which pose complex challenges when applied to algorithmic decision-making systems. Can AI reliably distinguish combatants from civilians? Who is responsible when an autonomous system causes unlawful harm? What legal status do machine-generated decisions have under the laws of armed conflict? The talk also addresses regulatory gaps and the need for legal adaptation in response to rapidly evolving AI capabilities. It evaluates existing national and international initiatives, such as the UN Group of Governmental Experts (GGE) on LAWS, and considers how soft law, codes of conduct, and arms control regimes might supplement traditional legal tools. Finally, it offers policy recommendations for states, military organizations, and the tech industry to ensure the development and deployment of AI in warfare remains legally compliant, ethically sound, and under meaningful human control.
mgr Maciej Czyszczoń	*Artificial Intelligence as a Moral Agent? Challenges and Implications of James Moor's Classification*	The continuous development of artificial intelligence (AI) raises significant philosophical and ethical questions concerning its capacity to be regarded as a moral agent. James Moor's typology systematically classifies moral agency within artificial entities, proposing four categories: ethical impact agents, implicit ethical agents, explicit ethical agents, and full ethical agents. This presentation aims to analyze and critically assess these categories, clarifying their theoretical foundations and exploring representative examples from current technological applications. It further addresses central conceptual and practical challenges associated with assigning moral agency to AI, incorporating insights from contemporary philosophical critiques by scholars such

		as Joanna Bryson, Luciano Floridi, Mark Coeckelbergh, and others. The concluding remarks highlight the relevance of Moor's typology to ongoing ethical debates in applied domains, notably autonomous transportation systems, and AI-assisted medical decision-making, while also identifying open-ended questions for future research regarding the potential evolution of machine moral autonomy.
mgr Dawid Trela	*Artificial Intelligence in Financial Security: Legal Challenges in Japan's AML/CFT Regime and Comparative Insights from Selected EU Countries*	The presentation explores the legal aspects of applying artificial intelligence (AI) in Japan's anti-money laundering and counter-terrorist financing (AML/CFT) system. It highlights key regulatory challenges and contrasts them with selected solutions adopted in EU member states—Germany, France, and Poland. The analysis includes a detailed review of national legislation, case law, legal scholarship, and regulatory guidelines, focusing on liability for AI-driven decisions, personal data protection, and compliance with FATF standards. Particular attention is paid to existing regulatory gaps in Japan, with legislative recommendations proposed in light of European experiences—especially concerning algorithmic transparency and safeguards for clients' personal data. The practical insights aim to inform the development of future regulatory frameworks for AI use in the financial security sector, balancing the protection of fundamental rights with international AML/CFT obligations.
Panel 3: AI in Military and Defence Applications **10:00 – 12:00** **Link: https://tinyurl.com/5n7puk5m**		
prof. Anastasios-Nikolaos Kanellopoulos	*Integrating AI into Counterintelligence: A New Security Paradigm*	Counterintelligence (CI) and Artificial Intelligence (AI) represent two distinct yet increasingly interconnected domains critical to national and international security. CI encompasses activities designed to detect, prevent, and counter hostile intelligence efforts, such as espionage, sabotage, and unauthorized information gathering. In parallel, AI refers to advanced computational systems capable of performing tasks traditionally requiring human intelligence, including learning, reasoning, and problem-solving. This paper explores the transformative impact of AI on CI practices, highlighting how AI technologies are reshaping national security strategies through enhanced data analysis, threat detection, and predictive capabilities. The discussion delves into the dynamic interplay between CI and AI, examining both the opportunities and challenges that arise from their convergence. It underscores the necessity of leveraging AI to bolster CI operations amidst evolving global threats, while critically addressing the ethical dilemmas and privacy concerns inherent in AI's deployment within intelligence frameworks. To

		provide concrete illustrations of these dynamics, this paper presents a series of international case studies. These cases will demonstrate real-world applications of AI in CI, showcasing the diverse approaches adopted by leading nations. Specifically, we will conduct a comparative analysis focusing on the integration of AI in CI strategies across the United States, China, Russia, and Israel. Each case will dissect the specific methodologies, strategic implementations, and the unique challenges faced by each nation. Ultimately, the paper emphasizes the dual imperative for intelligence agencies and policymakers: to harness AI's potential effectively for CI while safeguarding democratic values, privacy rights, and ethical standards. Striking a balance between technological advancement and responsible governance is paramount in navigating the future landscape of national security. The case studies will serve to underline the importance of this balance, highlighting both successful implementations and cautionary tales, and providing valuable insights for future policy development.
inż. Paweł Jaskuła **inż. Maria Kamińska**	*Utilizing AI for Military Operational Planning and Simulation*	The dynamic growth of artificial intelligence (AI) is leading to its use in many areas, including the military. As AI systems continue to advance at handling complex data, recognizing patterns, and helping with decisions, they are becoming important tools for national security and defense. Modern armies use AI to work more efficiently, understand situations better, and handle the complicated nature of today's conflicts. Machine learning, predictive models, and smart decision-making systems help provide faster and more accurate assessments, allowing for better and quicker responses. One of the most promising areas for AI is military planning and simulation. AI-powered virtual environments let military teams test strategies, predict outcomes, and improve their tactics in a controlled, risk-free setting. These simulations help train soldiers and assist in planning missions by giving commanders data-based insights into different options. AI also helps improve logistics, analyze intelligence, and detect threats, all of which boost military readiness. This paper addresses the use of AI in the planning and simulation of military operations. It presents a review of current applications of artificial intelligence in virtual military simulations, highlights the benefits of their implementation for decision-making processes and operational readiness, and discusses challenges like security, ethics, and system reliability. The goal is to indicate possible directions for future research and present how AI can be used in national defense systems.
Lt. PhD Iwona Szkudlarek	*Professional Development of Soldiers: Immersive*	The growing influence of artificial intelligence (AI) in cybersecurity has given rise to both new opportunities and new risks, with generative AI (GenAI) playing a particularly transformative

	Technologies in Teaching Military English	role. This review examines the evolving impact of generative AI technologies in cybersecurity, analysing their dual use in enhancing defensive capabilities and enabling novel attack vectors. Drawing on an extensive body of scientific literature published between 2017 and 2025 - with 2017 marking the introduction of the Transformer architecture that underpins modern large language models (LLMs), sourced from major digital libraries, the review identifies key trends in the application of GenAI to cybersecurity. It explores how new tools such LLMs and platforms like ChatGPT are increasingly utilised for phishing, adversarial attacks, automated hacking, and malware generation. Simultaneously, the study highlights the growing adoption of GenAI in threat detection, code analysis, and cyber defence automation. Furthermore, the review discusses the intersection of emerging AI applications with cybersecurity risk management frameworks and regulatory standards, including NIS2, the NIST AI Risk Management Framework, and relevant ISO/IEC standards (22989, 23053, 23984, and 42001). By synthesising current research and regulatory developments, this article underscores the pivotal role of generative AI in shaping the future landscape of cybersecurity and emphasises the urgent need for innovative defensive strategies in an increasingly cloud-dependent digital environment.
dr Krzysztof Pająk	*Enhancing Maritime Infrastructure Security through AI-Driven Naval Drone Operations in the Southern Baltic*	The integration of artificial intelligence in naval drones, especially autonomous ones, to enhance the security of maritime infrastructure is becoming essential to effectively protect maritime infrastructure. AI's role in drones' operations encompasses threat detection, real-time decision-making, and autonomous navigation. Providing a near real-time, reliable, and 24/7 proactive approach to protecting ports, offshore platforms, and underwater assets may be the only adequate response to the growing range of maritime threats.
PhD Candidate Sunny Anand	*Role of AI in Modern War*	The Evolving Role of Artificial Intelligence in Modern Warfare This research paper explores the transformative impact of Artificial Intelligence (AI) on the landscape of modern warfare. From enhancing strategic autonomy and decision-making to enabling the deployment of sophisticated unmanned systems across air, land, and sea, AI is rapidly reshaping military capabilities and doctrines. This study examines the specific applications of AI in areas such as intelligence analysis, target recognition, cyber warfare, and logistics, highlighting the potential for increased efficiency, reduced human risk, and the acceleration of operational tempos. However, the integration of AI into military domains also raises critical ethical and legal concerns, particularly regarding accountability, human control over lethal autonomous weapons, and adherence to international law. This paper delves into these challenges, analyzing the strategic and tactical

		implications of AI-driven warfare and considering future trends such as human-machine teaming and the integration of advanced machine learning techniques. Ultimately, this research aims to provide a comprehensive understanding of the evolving role of AI in modern conflict, its potential benefits and risks, and the crucial considerations for navigating this technological revolution in the realm of defense.
mgr Patryk Niksa	*Military Applications of Artificial Intelligence*	My presentation will focus on military applications of AI. The speech will address 3 concepts of using artificial intelligence (human in the loop, human on the loop, human out of the loop). With the ability to process large amounts of data, analyze complex patterns and make instant decisions, artificial intelligence is revolutionizing military technology. The application of artificial intelligence in the military area in particular concerns C5ISTAR, autonomous combat systems, intelligent decision-making systems, cyberspace defense systems, reconnaissance and intelligence systems, support for logistics operations, simulation training systems.
Kamil Jan Margielewicz	*Selected Automatic Weapon Systems of NATO Member States: Context of AI Application*	During my speech, I would like to present issues related to the use and application of artificial intelligence in selected weapon systems used by the armies of NATO member states. I am leaning towards such a topic due to the development of artificial intelligence, the current geopolitical situation in the world, and my own interest in the subject. I would present aspects related to the specific installation of artificial intelligence in selected weapon systems. I would focus mainly on air defense systems, aimed at intelligently shooting down enemy objects violating NATO airspace. I would show specific examples of how artificial intelligence can be used, and I would present the positive and negative aspects of the implications of such solutions in matters of national security. I would also show the profitability side of such ventures, in financial terms. I would present the issues related to training an anti-aircraft launcher operator and installing systems using artificial intelligence - a comparison of profitability. In the final few sentences, I presented the potential threats that may arise due to losing control over a solution or system using artificial intelligence.
Panel 4: AI for Cybersecurity: Defending Critical Systems and Infrastructure **12:00 – 14:00** **Link: https://tinyurl.com/2sx9ysjb**		
PhD Pedro Silva	*AI-Driven Cybersecurity:*	As artificial intelligence (AI) continues to revolutionize cybersecurity and critical infrastructure

Baptista	*Balancing Innovation, Security, and Ethical Challenges in Critical Infrastructure Protection*	protection, it presents both unprecedented opportunities and complex challenges. This paper explores the dual role of AI as both an enabler of advanced security mechanisms and a potential vector for emerging cyber threats. By analyzing AI-driven threat detection, predictive analytics, and autonomous response systems, we examine how these technologies enhance resilience against cyberattacks. However, the increasing reliance on AI also raises concerns about algorithmic bias, privacy risks, and vulnerabilities that adversaries may exploit. Additionally, we assess the ethical and policy considerations surrounding AI deployment in security frameworks, particularly in military and national defense contexts. Through case studies and real-world applications, this research provides insights into the evolving intersection of AI, cybersecurity, and infrastructure protection, highlighting the need for robust governance and international collaboration.
prof. George Zombanakis, prof. Vasileios Symeonidis	*Defending Defence: The Demand for Cybersecurity Expenditures by the Hellenic MOD*	This paper represents one of the early attempts to approach the issue of the demand for cybersecurity funds by the Hellenic Department of Defence. What we do, in fact, is outline the cybersecurity issue for the Hellenic Defence sector and the problems arising following the increasing cyberattacks in the international environment and the ensuing risk for breaches. We then propose a theoretical background, based on which we formulate a demand for cybersecurity funds required to face such threats. Based on this background we estimate a demand function for such funds and discuss their degree of responsiveness to changes of its determinants, like the threats facing the Hellenic Defence sector and the funds required to promote and enhance similar efforts. The last part of the paper involves policy implications and conclusions, as well as future research suggestions.
Cmdr. Amila Prasanga	*Leveraging AI for Subsea Cable Protection: Maritime Security Imperatives for Sri Lanka and Vulnerable Island States*	Submarine cables are critical to global communications, transmitting over 95% of international internet traffic and economic transactions. For island states such as Sri Lanka, which depend heavily on uninterrupted digital connectivity for economic growth, national security, and regional cooperation, the protection of submarine cable infrastructure has become a vital maritime security concern. The vulnerabilities of these subsea assets are increasingly exposed to both natural hazards and anthropogenic threats, including grey-zone tactics—attacks by non-state actors acting on behalf of state interests. Such tactics pose growing threats to critical subsea infrastructure, often in contested maritime zones, where traditional security measures are insufficient. This research explores the potential for integrating Artificial Intelligence (AI) into submarine cable protection strategies, with a specific focus on the security challenges faced by

		Sri Lanka and other vulnerable island states in the Indian Ocean Region (IOR). The study applies a multidisciplinary approach, combining qualitative research, geospatial analysis, case studies, and expert interviews. It draws on existing maritime security theories, critical infrastructure protection frameworks, and emerging AI applications, including machine learning-based anomaly detection, autonomous underwater vehicles (AUVs), and AI-powered satellite imagery. This methodology is employed to map key submarine cable landing points, assess high-risk maritime zones, and identify gaps in current protective frameworks. The growing influence of grey-zone tactics, which often involve indirect state actions to disrupt or damage infrastructure, is examined as a primary threat to subsea security. The study underscores the need for innovative security measures to counter these non-traditional and increasingly sophisticated threats. The research finds that Sri Lanka's existing legal, institutional, and technical frameworks are inadequately prepared to handle hybrid maritime threats targeting subsea infrastructure. Despite its strategic location in the IOR, the nation's naval and coastal surveillance systems lack the integration of AI and predictive capabilities, leaving critical infrastructure vulnerable to covert attacks. Furthermore, inter-agency coordination and international cooperation on subsea security remain limited. By evaluating AI solutions used by other island and coastal states, the study proposes a strategic roadmap for Sri Lanka, which includes the establishment of a national subsea infrastructure security task force, the integration of AI-based surveillance and monitoring systems, and the formulation of a national policy on digital infrastructure protection in the maritime domain.
dr Karol Chlasta	*Generative AI in Cybersecurity: Emerging Threats, Defensive Strategies, and Standards*	The growing influence of artificial intelligence (AI) in cybersecurity has given rise to both new opportunities and new risks, with generative AI (GenAI) playing a particularly transformative role. This review examines the evolving impact of generative AI technologies in cybersecurity, analysing their dual use in enhancing defensive capabilities and enabling novel attack vectors. Drawing on an extensive body of scientific literature published between 2017 and 2025 - with 2017 marking the introduction of the Transformer architecture that underpins modern large language models (LLMs), sourced from major digital libraries, the review identifies key trends in the application of GenAI to cybersecurity. It explores how new tools such LLMs and platforms like ChatGPT are increasingly utilised for phishing, adversarial attacks, automated hacking, and malware generation. Simultaneously, the study highlights the growing adoption of GenAI in threat detection, code analysis, and cyber defence automation. Furthermore, the review

		discusses the intersection of emerging AI applications with cybersecurity risk management frameworks and regulatory standards, including NIS2, the NIST AI Risk Management Framework, and relevant ISO/IEC standards (22989, 23053, 23984, and 42001). By synthesising current research and regulatory developments, this article underscores the pivotal role of generative AI in shaping the future landscape of cybersecurity and emphasises the urgent need for innovative defensive strategies in an increasingly cloud-dependent digital environment.
mgr Marceli Hązła	*Quantum Technology as a Determinant of Cybersecurity and Technological Sovereignty of the European Union*	In the third decade of the 21st century, much of the public attention has been focused on the development of Artificial Intelligence (AI) and its possible impact on economies, societies and nation states. Historically, achieving a sufficient level of computing power has been a major limiting factor in the development of AI, but over the past decade, the number of computations used to train leading-edge artificial intelligence systems has increased 350 million times, enabling ground-breaking models such as ChatGPT, DALL-E and DeepSeek. However, quantum technology is emerging on the horizon which could completely reformulate previous paradigms of technological development as it will offer a level of computational complexity unattainable with traditional silicon processors. In traditional silicon-based microprocessors, the increase in computing power depends primarily on the number of transistors, which only operate on values of 0 and 1. Meanwhile, qubits, which are the quantum equivalent of a transistor, can take on any state between 0 and 1, increasing their computing capabilities by tens of orders of magnitude. For example, a quantum computer would be able to solve in one day a problem that would take a traditional silicon supercomputer more time than has passed since the Big Bang. This means that access to quantum technology will become one of the fundamental determinants of national security in the coming years. This is because quantum computers will make existing cryptographic methods obsolete and unreliable for data confidentiality. In addition to this, they will also dramatically increase the productivity of economies, taking the quality of the management of supply chains, investment portfolios or the processes of designing new drugs to unprecedented levels. Unlike silicon chips, whose market is dominated by Taiwan and the US, countries such as China (US$15.3 billion), Germany (US$5.2 billion), and the UK (US$4.3 billion) are leading the way in investment in quantum technology. This means, therefore, that quantum technology represents an opportunity for EU member states to break out of the trap of dependence on Taiwanese and US semiconductors, and that its development will therefore be crucial to achieving technological sovereignty for the Old Continent. The presentation is divided

		into three parts. The first considers the geopolitical and economic conditions of the market for traditional silicon microchips. The second part compares the computational capabilities of quantum technology with existing silicon technology and describes its most important applications. Finally, part three presents the issue of quantum technology development in the context of technological sovereignty of the European Union. The presentation uses literature analysis, statistical data analysis and deductive reasoning. Due to the current nature of the issues analysed, it also draws on numerous internet sources.
Klaudia Banasiewicz	*AI in Cybersecurity: Innovations, Challenges, and Future Trends*	In an era of rapidly evolving cyber threats, artificial intelligence (AI) is playing an increasingly pivotal role in reshaping the cybersecurity landscape. This presentation will explore how AI is enhancing cybersecurity through automation, predictive analytics, and intelligent threat detection. We will delve into the latest advancements, including AI's ability to combat zero-day attacks, detect malware with high accuracy, and respond to breaches in real time. Furthermore, we will explore the newest trends in AI-powered cybersecurity for 2025, such as the integration of AI with cloud security, the rise of autonomous security systems, and the use of deep learning models for advanced attack prevention. Special attention will be given to challenges, including the ethical implications, the risk of adversarial AI, and how businesses can balance innovation with security. By the end of the presentation, participants will understand both the potential and the risks of AI in cybersecurity, offering insights into the future trajectory of this cutting-edge field.
Wiktor Wilkołaski	*Towards Quantum-Resilient Systems: Introducing the AI-Enhanced Cryptographic Agility Framework (AI-ECAF) Empowered by Post-Quantum Cryptography*	Cryptographic agility—the ability of a system to swap cryptographic algorithms and parameters rapidly in response to emerging threats—is crucial for securing information systems against powerful cyberattack tools. This research proposes a concept of AI-Enhanced Cryptographic Agility Framework (AI-ECAF) to future-proof systems against both quantum computing threats and AI-powered attacks. Research first surveys the threat landscape: quantum algorithms (e.g. Shor's and Grover's) threaten current public-key (asymmetric) and symmetric ciphers. At the same time AI and machine-learning techniques accelerate cryptanalytic and side-channel attacks (e.g. neural-network-based key recovery). In the next part research mentions related work on crypto-agility, post-quantum cryptography, and machine learning in security, noting that agility concepts are gaining eminence, but still lack consensus definitions. Existing agility frameworks and post-quantum proposals (e.g. the recent CSWP 39 and systematic reviews on cryptographic agility) provide groundwork but lack unified approach and AI integration. The proposed

		framework integrates real-time threat intelligence, a machine-learning decision engine, and a modular crypto library. In proposed framework architecture, an AI module continuously analyzes threat data and usage patterns to recommend or automatically trigger algorithm updates or key rotations and adapt to current standards and organization policies. Detailed case studies illustrate deployment scenarios: (1) an enterprise key-management system automating migration to hybrid classical/PQC suites (2) an IoT device network adapting encryption in resource-constrained environments. Research also discuss legal and regulatory aspects (e.g. acts and documents issued by international bodies and organizations) that influence "agile" design choices. Finally, Research outlines future research directions, including adversarial robustness for AI decision engines, formal metrics of agility, and integration with upcoming standards. The results show that AI-assisted agility can greatly shorten response times to vulnerabilities and maximize resilience against next-generation attacks.
Islam Hajiyev	*The Role of Quantum Technologies in Future Cybersecurity Strategies*	The rapid advancement of quantum technologies poses both significant opportunities and threats to the field of cybersecurity. While quantum computing has the potential to break widely used cryptographic algorithms, it also introduces innovative methods for securing communication, such as quantum key distribution. This presentation explores the dual nature of quantum technologies in the context of cybersecurity strategies, particularly focusing on the transition from classical to post-quantum cryptographic systems. The talk will discuss current developments in quantum cryptography, the anticipated timeline for practical quantum computing, and the implications for national and international security infrastructures. Emphasis will also be placed on the need for proactive measures, including the integration of quantum-resistant algorithms, policy development, and interdisciplinary collaboration. By addressing both the challenges and benefits of quantum technologies, this presentation aims to contribute to a comprehensive understanding of their role in shaping the future of cybersecurity.

Closing:

14:30 – 15:00
Link: https://tinyurl.com/5n7puk5m
prof. Bert Chapman, Purdue University, USA, *Selected Artificial Intelligence Provisions in U.S. Fiscal Year 2025 National Defense Authorization Act*

The 2025 Fiscal Year National Defense Authorization Act contains multiple provisions relating to artificial intelligence (AI). These congressionally mandated provisions direct various sections of the Department of Defense (DOD) and individual U.S. armed service branches to execute congressional

intent for AI policymaking. Examples of such intent include identifying and planning DOD's AI workforce, demonstrating AI biotechnology applications for national security, improving the human usability of AI systems, and establishing an AI security center. This presentation will note that reports on these initiatives must be prepared for relevant congressional oversight committees and, in many cases, publicly released within specific time frames and that ongoing oversight of these programs will engage in by congressional committees and other federal agencies.