SECURITY & DEFENCE QUARTERLY
https://securityanddefence.pl/

Introduction to the Special Issue on AI frontiers in cybersecurity and infrastructure protection

Abdellah Chehri

https://orcid.org/0000-0002-4193-6062

Royal Military College of Canada, 13 General Crerar Crescent, Kingston, ON K7K 7B4, Canada

Citation: Chehri, A. (2025) 'Introduction to the Special Issue on AI frontiers in cybersecurity and infrastructure protection', *Security and Defence Quarterly*, 52(4), pp. 1–3. doi:10.35467/sdq/217647.

Published: 31 December 2025

Artificial intelligence (AI) is rapidly reshaping the global security architecture, influencing military capabilities, social dynamics, and international cooperation. As these transformations accelerate, the necessity to reevaluate traditional security paradigms becomes increasingly urgent. Contemporary security challenges extend far beyond physical threats, encompassing a broader spectrum of cyber and informational risks that demand innovative adaptive responses.

Artificial intelligence offers both unprecedented opportunities and complex risks. On the one hand, it enables predictive analytics, autonomous decision-making, and enhanced resilience across critical infrastructures; on the other hand, it raises concerns about privacy, civil liberties, and the ethical deployment of autonomous systems. The integration of AI into cybersecurity and infrastructure protection requires strategies that are technologically advanced, socially responsible, and globally coordinated.

For example, AI-driven cybersecurity measures can detect and neutralise threats in real time, safeguarding essential services such as healthcare, transportation, and energy. AI applications in engineering and infrastructure can strengthen resilience against both natural and human-made disruptions. Yet, these advances must be balanced with careful consideration of ethical implications, policy frameworks, and the risks of misuse from autonomous weapon systems to disinformation campaigns that destabilise societies.

To address these evolving complexities, *Security and Defence Quarterly* is publishing a Special Issue entitled *AI frontiers in cybersecurity and infrastructure protection.* This issue presents original research that advances the transition from traditional security models to comprehensive strategies capable of meeting the challenges of AI and cyber threats.

By fostering collaboration across disciplines, it highlights the transformative role of AI in shaping secure, resilient, and inclusive societies. Through rigorous research and innovative perspectives, it outlines a path towards a security architecture that is adaptive, ethical, and prepared for the challenges of tomorrow.

The special issue on *AI frontiers in cybersecurity and infrastructure protection* has received a remarkably high number of submissions, underscoring the growing global interest in the role of AI in reshaping security paradigms and safeguarding critical infrastructures. The accepted contributions span a wide spectrum of themes, including strategic analyses of cyber conflicts, AI-driven approaches to financial security, regulatory and ethical challenges of AI as a moral agent, applications of autonomous systems in maritime defence, and the dual-use dilemma of generative AI in cybersecurity. Together, these papers ensure accessibility and relevance to the broader security and defence research community while offering diverse insights into the technological, legal, and strategic dimensions of AI in contemporary security.

In "The dual-use dilemma of generative artificial intelligence in cybersecurity: Navigating the explosive growth in offensive and defensive applications," the author provides a systematic review of 3,389 publications on AI in cybersecurity, with a focus on generative techniques, such as large language models (LLMs). The analysis reveals an explosive rise in generative AI (GenAI) research since 2022, identifying dominant themes, including LLMs, blockchain, cyberattacks, generative coding, smart energy/internet of things (IoT), and malware. Findings highlight the dual-use dilemma, as malicious actors exploit GenAI for offensive purposes while defenders develop it to strengthen cybersecurity. The study underscores the urgent need for organisations to secure cloud and edge systems and enhance staff capabilities in threat detection and response using GenAI-driven methods.

Using a game-theoretic lens, "Strategic analysis of cyber conflicts: A game-theoretic modelling of global cyber crises in the 2000s" examines eight case studies of interstate cyber conflicts, modelling actors, strategies, and outcomes to identify Nash equilibria. It reveals recurring dynamics, such as aggressor states favouring denial strategies, victims responding with retaliation, and election-related cyber operations driving instability. By introducing a novel analytical framework, the study demonstrates the value of game theory in forecasting state behaviour in cyberspace and offers practical insights for policymakers and scholars in cybersecurity and international relations.

Through the case study presented in "Technological maturity for Jeune École: The case of Ukraine's naval strategy," the authors analyse how Ukraine shifted the balance of power in the Black Sea through the combined use of anti-ship cruise missiles, aerial drones, and maritime drones. Using process tracing, the study shows that traditional weaponry enabled initial sea denial, while unmanned systems later consolidated and extended control. Findings highlight that even smaller states can achieve significant strategic effects by leveraging modern technologies within the historic Jeune École doctrine. The research underscores how technological advances have mitigated the limitations of small platforms, offering a blueprint for asymmetric maritime strategies against superior naval forces.

Focusing on the protection of critical maritime assets, "Enhancing maritime infrastructure security through AI-driven naval drone operations in the Southern Baltic Sea" explores the role of AI-supported autonomous systems in protecting critical maritime assets, such as ports, offshore platforms, subsea cables, and pipelines. Using a qualitative analytical approach, the study identifies key patterns and trends in maritime security under conditions of spatial congestion and geopolitical risk. Findings show that AI-enhanced naval drones enable continuous, real-time monitoring and faster threat detection, thereby

strengthening resilience against hybrid threats. The research underscores that integrating AI and autonomous systems into maritime operations is essential for safeguarding infrastructure, ensuring stability, and reinforcing national defence in the rapidly evolving Baltic Sea region.

At the level of institutional cybersecurity practice, "Cybersecurity and incident response processes for maintaining operational security and continuity at vocational education institutions" examines how staff in Finnish vocational schools handle suspected cybersecurity incidents. Using qualitative interviews, the study reveals that while formal reporting procedures exist, staff often relies on informal networks and direct information technology (IT) contact, with urgent cases communicated by phone. This approach, although efficient, limits documentation and post-incident learning. The research underscores the need to integrate structured digital tools with flexible, human-centred communication methods to strengthen resilience, protect sensitive data, and ensure continuity in vocational education environments.

Adopting a doctrinal and comparative legal approach, "Artificial intelligence in financial security: Legal challenges in Japan's AML/CFT regime and comparative insights from selected EU countries" analyses regulatory gaps in deploying AI for anti-money laundering (AML) and counter-terrorist financing (CFT) systems. Using doctrinal legal analysis and comparative methodology, it assesses alignment with the Financial Action Task Force (FATF) recommendations, the General Data Protection Regulation (GDPR) and the EU Artificial Intelligence (AI) Act across Japan, Germany, France, and Poland. Findings reveal fragmented frameworks, liability concerns, and tensions between transparency and tipping-off, with Germany and France showing stronger supervisory maturity than Japan and Poland. The study highlights the need for governance-heavy, auditable, human-in-the-loop designs and offers best practices for aligning AML, AI, and data-protection regimes to safeguard both effectiveness and fundamental rights.

Engaging with longstanding debates on machine ethics, "Artificial intelligence as a moral agent: Regulatory implications and a relational–contextual extension of Moor's classification" reassesses James Moor's typology of machine morality in light of the European Union's (EU) AI Act and liability directives. It introduces a novel relational–contextual dimension and a three-factor Responsibility Index (RI_3) that cross-classifies AI systems by complexity, autonomy, and predictability, offering lawmakers a pragmatic regulatory tool. Findings confirm Moor's framework as a valuable baseline but argue it must be augmented to address accountability gaps in large-scale autonomous AI. The study bridges analytic philosophy and policy, aligning moral agency debates with concrete legal duties in socio-technical networks.