Original Scientific Paper/Original naučni rad UDC/UDK: 341:004.8
Paper Submitted/Rad primljen:31.12.2025.
Paper Accepted/Rad prihvaćen:10.01.2026.
DOI: 10.5937/SJEM2601101S

Digitalni *jus pacis*: međunarodna saradnja i pravni temelji mira u doba veštačke inteligencije

Troy Smith[1], Mikhail Byng[2]

[1] Ministry of Homeland Security, Trinidad and Tobago, dr.troy.smith@outlook.com
[2] University of the West Indies, Trinidad and Tobago, byngmikhail@gmail.com

Abstract: Rad razmatra transformativni uticaj veštačke inteligencije (VI) na globalnu bezbednost, kao i postojeće praznine u zakonodavnim okvirima za upravljanje sve izraženijim pretnjama u ovoj oblasti, naročito ograničenu sposobnost da se na adekvatan način reguliše tzv. „algoritamsko ratovanje". U radu se uvodi koncept *digitalnog jus pacis* kao novog pravno-etičkog okvira usmerenog na očuvanje mira u eri veštačke inteligencije. Ovaj koncept se nadovezuje na *jus ad bellum* i *jus in bello*, uz poseban naglasak na sprečavanje digitalne eskalacije, obezbeđivanje odgovornosti i zaštitu ljudskog dostojanstva u sajber prostoru. Uzimajući u obzir geopolitički i strateški kontekst u kojem se ove tehnologije razvijaju, rad predlaže tri ključna stuba algoritamskog mira: (1) zakonit dizajn (ljudski nadzor i proporcionalnost); (2) kooperativno upravljanje (regionalno i globalno usklađivanje); i (3) moralno uzdržavanje (digitalna humanitarna etika). Cilj rada je da se koncept digitalnog *jus pacis* razvije i pozicionira kao temeljni princip savremenog međunarodnog prava, čime bi se postavila osnova za budući Sporazum o miru u oblasti veštačke inteligencije ili za njegovu integraciju u Globalni digitalni sporazum Ujedinjenih nacija (GDC).

Ključne reči: veštačka inteligencija; algoritamsko ratovanje; digitalni *jus pacis*; globalno upravljanje; regulatorni okvir

Digital Jus Pacis: International Cooperation and Legal Foundations for Peace in the Age of Artificial Intelligence

Abstract: This paper aims to explore the transformative effect of artificial intelligence (AI) on global security and the existing gaps within legislative frameworks for managing the growing threats in this area, particularly the inability to manage "algorithmic warfare." Introducing the concept of a digital jus pacis, a new legal-ethical framework for preserving peace in the AI era. This proposed concept builds upon jus ad bellum and jus in bello, focusing on preventing digital escalation, ensuring accountability, and protecting human dignity in cyberspace. Whilst accounting for the geopolitical and strategic context within which this new technology is being developed, the article proposes three pillars for algorithmic peace, these include: 1) Lawful design (human oversight and proportionality); 2) Cooperative governance (regional and global alignment); 3) Moral restraint (digital humanitarian ethics). The goal is to develop and position the concept of digital jus pacis as a core principle of modern international law, which lays the foundation for a future AI Peace Compact or integration into the UN Global Digital Compact (GDC).

Keywords: Artificial Intelligence; Algorithmic Warfare; Digital Jus Pacis; Global Governance; Regulatory Framework

1. Introduction

Artificial intelligence (AI) is rapidly transforming global security, from autonomous weapons systems (AWS) and AI-driven security and intelligence analysis to cognitive warfare and information operations. The growth of AI and its integration into critical sectors within both the public and private sectors increases the importance of understanding this new technology and its potential impact on the world. These developments have already begun to reshape how conflict is waged, how threats are perceived, and how states and non-state actors compete in both physical and digital domains. The speed, opacity and scale of these AI-enabled capabilities also expose deep gaps in existing legal and regulatory frameworks, particularly those governing the lawful use of force, accountability,

and international cooperation. It appears that AI is advancing at such a rapid rate that regulatory frameworks are unable to adjust adequately or in a timely fashion to prevent the unfolding of worst-case scenarios or less desirable outcomes.

Classical *Just War* doctrines, such as *jus ad bellum* and *jus in bello*, which were primarily developed in relation to kinetic warfare, struggle to address algorithmic targeting, weaponised data, and AI-driven escalation dynamics (Bode & Bhila, 2024; Smith, 2025a). At the same time, new global governance initiatives are emerging to regulate AI more broadly, including the European Union AI Act, the Council of Europe's Framework Convention on AI, the United Nations Secretary-General's High-Level Advisory Body on AI, the United Nations Independent International Scientific Panel on Artificial Intelligence, and regional frameworks in Latin America and the Caribbean (European Parliament, 2024; ECLAC, 2024; United Nations High-Level Advisory Body on AI, 2024). However, the regulation of AI qualified by the need to present stymying innovation has not yet reached a nexus of the required understanding and applicability of controls for AI use in conflict.

Furthermore, whilst much of the academic and policy attention is placed on the strategic competition between the United States (US) and China in relation to technological progress in the domain of advanced technologies, middle powers and smaller states are actively engaging in these areas, further heightening the need for frameworks to guide the development and application of these new technologies. Countries such as Singapore, Norway, the United Kingdom, Turkey, Israel and others are actively making rapid progress in the field, further emphasising the need for collective and global action (Ratska & Bitzinger, 2023). What normative guidelines, legislative frameworks, and laws exist to address the paucity of guardrails regarding these new technologies? Furthermore, what recommendations can be put forth to address the absence of regulations and rules that provide a common ground for states and even private sector entities to engage AI tools? The importance of the answers to these questions is not in the development of country or region-specific solutions but in the applicability on the global scale to maintain peace through alignment with existing anti-war, just war, and humanitarian frameworks

Despite the proliferation of AI ethics guidelines, policy statements, and emerging regulatory instruments, there is an absence of coherent peace-oriented legal frameworks specifically designed to prevent AI-driven conflict/escalation prior to the outbreak of hostilities. Against this backdrop, the concept of *digital jus pacis* provides a means to extend peace-oriented legal thinking into the digital and algorithmic realm. Rather than focusing solely on the conditions under which force may be used (*jus ad bellum*) or how it should be constrained once conflict has begun (*jus in bello*), *digital jus pacis* foregrounds the law and norm-building required to prevent AI-driven escalation, protect human dignity, and preserve the informational and cognitive foundations of peace. Notably, international cooperation is increasingly subjugated to the narrow realist political and economic considerations of nations which maintain the capacity to affect the direction of development in the field. Hence, the need to emphasise international cooperation, particularly in selective domains of high impact. This is essential even in times of international flux, increased geopolitical tensions and political uncertainty, as a lack of guardrails in these areas will likely lead to further uncertainty and costly unintended consequences (Dookeran & Byng, 2025). In response, this paper seeks to address the existing gap by advancing *digital jus pacis* as a distinct and necessary complement to existing just war doctrines and contemporary AI governance regimes.

2. Key Definitions and Conceptual Frameworks

2.1. Jus ad Bellum, Jus in Bello and Jus Ante Bellum

At the core of the discussion on the ethics of warfare is the concept of "Just War," which provides a lens for assessing the justification for and conduct of warfare (Hidalgo, 2025). Perhaps at its core, the concept aims to reduce the likelihood of escalation, damage, or incidental harm that could result from war, and provide an avenue to return to a peaceful state, rather than justifying any war as "just" (Hidalgo, 2025; Smith, 2025a).

Jus ad bellum governs the conditions under which states may resort to force, focusing on self-defence, proportionality and the authority to use force under the UN Charter. *Jus in bello* (international humanitarian law) regulates how force must be exercised once conflict has begun, including the principles of distinction, proportionality and precaution.

However, AI challenges both bodies of law. Algorithmic escalation can blur thresholds for armed attack; cyber operations may fall below traditional conceptions of "force"; and cognitive warfare can destabilise societies without firing a shot. In this context, some scholars and practitioners have proposed *jus ante bellum*: a set of norms and obligations that focus on prevention, risk reduction, and pre-emptive transparency to avoid conflict spirals in the first place (Nishimoto, 2025). This doctrine resonates with the concept of jus pacis presented in this paper.

2.2. Digital Jus Pacis

The proposed concept of *digital jus pacis* seeks to extend existing doctrines into the digital domain. It is not simply an AI-specific law of armed conflict, nor merely another set of ethical guidelines. Digital *jus pacis* is proposed not as a replacement for existing international legal regimes, nor as an immediately binding body of law, but as a normative-legal framework. Its introduction seeks to embed peace-preserving principles into the design, deployment and governance of AI systems that affect international security by providing a framework that guides state behaviour, informs treaty development, and shapes the interpretation of existing obligations in contexts where AI-enabled capabilities risk destabilising peace before the threshold of armed conflict is reached.

Three pillars, which will be further explained later in this paper, underpin this framework:

1. Lawful design
2. Cooperative governance
3. Moral restraint

In this way, *digital jus pacis* treats AI as a domain in which legal, technical and normative architectures must converge to prevent algorithmic escalation and preserve human dignity.

3. The Geopolitical and Strategic Context of AI

A consensus exists that the US and China are in direct competition regarding progress in several areas, including advanced technologies, particularly AI. The vast investments by these two countries in both the commercial and public sectors, the increasing sensitivities regarding commercial espionage, and the emphasis on AI supply chains (particularly regarding rare earth minerals essential to the computing power required by AI tools), illustrate the high value placed on AI. However, other influential states are actively investing to ensure they remain at the cutting edge of new advancements in AI. Their collective actions, including he normative guardrails (or absence thereof) that they institute in particular, will likely prove highly consequential in determining the growth of the sector. As early as 2018, France, for example, commenced an investment scheme in which the government allocated $1.85 billion (USD) to AI technology, with similar efforts underway in the United Kingdom and Australia (Barsade & Horowitz, 2018). Other countries, including Türkiye, Norway, and Singapore, are investing substantially in their own AI infrastructure. These countries are attempting to utilise their existing relative advantages, such as strategic geographic location, foreign direct investment, and highly skilled labour forces, to leverage this new technology (Erai Türkiye, 2026; Barsade & Horowitz, 2018).

Similarly, the Israeli military, for example, has been actively utilising AI since 2014 in real-life applications, particularly in its 2014 conflict with Hamas, and in its more recent military activities in the Gaza Strip. The use of AI to analyse vast amounts of video footage and live feeds from hotspots around the Israeli border, throughout occupied territory and active battlefield operations, provides their security apparatus with the capacity to identify patterns, engage in predictive analytics, and take operational and tactical action accordingly (Lappin, 2017). The Israeli Defence Force (IDF) has signalled its intent to utilise AI tools not only for operational decision-making but also for strategic-level decision-making. This action will likely further enhance its military capacity by automating much of the time-consuming data collection and information sorting critical to high-level decision-making.

The application of AI to diverse sectors within the public and private domains will likely shape the geopolitical landscape of the 21st century. At the core of AI's hardware ecosystem are rare-earth elements (REEs). These elements are indispensable to key components and inputs which create the infrastructure upon which AI tools operate (Roy, 2025). Notably, these REEs are primarily extracted and refined by China, placing the country in a highly valuable position, at least in the short term, to determine the direction in which these resources are directed. Roy (2025) estimates that Beijing maintains 60% of control over extraction and 85% of refining capacity, notwithstanding the pre-eminence of private sector Taiwanese and US companies in creating the most advanced chips in the industry. The potential for geopolitical conflicts centred on access to these critical minerals may therefore become an increasingly significant feature of the 21st century's strategic landscape, a point already signalled by China's increasingly strategic posture toward Taiwan, which raise questions as to whether Beijing will eventually seek formal annexation or continue its consolidation of influence through diplomatic manoeuvring, economic leverage, and the mobilisation of international support.

For smaller states and middle powers, digital *jus pacis* offers more than an ethical framework. It provides a strategic instrument and foundational way of thinking that can shaping norms and future discussions in a domain traditionally dominated by technologically advanced actors. By embedding peace-preserving principles into AI

governance early, these states can exercise normative influence disproportionate to their material capabilities, reduce strategic vulnerability, and mitigate the risks of being norm-takers in algorithmic security environments. A concept well aligned with the global governance framework advanced by the established of the United Nations and actioned in initiative such as the Global Digital Compact and the Open-ended Working Group on security of and in the use of information and communications technologies.

4. Existing Legal and Governance Frameworks

4.1. International Humanitarian Law (IHL) and State Positions on Autonomous Weapons Systems (AWS)

International Humanitarian Law (IHL) applies to all means and methods of warfare, including those that rely on new technologies such as AI. The core principles of distinction, proportionality and precaution remain central, and states remain legally accountable for violations, regardless of the tools used (Viveros Alvarez, 2024). However, the integration of AI into targeting and decision-making processes creates practical challenges for compliance. Questions arise as to whether complex machine-learning models can reliably implement distinction; how proportionality assessments should be conducted when harm estimates are algorithmically generated; and how responsibility should be assigned when harm results from interactions between autonomous systems and human operators.

Several states and coalitions have issued political declarations on responsible military use of AI, setting out non-binding principles such as meaningful human control, reliability, and human accountability. These include national policy statements, regional initiatives and joint declarations in multilateral fora (Tréhu & Ricart, 2024; United Nations Secretary-General's High-Level Advisory Body on AI, 2024). While valuable, these efforts remain fragmented and lack the force of binding law.

4.2. Regional and Global AI Governance Instruments

A mix of binding regulations, soft-law instruments, and multistakeholder initiatives characterises the emerging global AI governance regime. Key examples include:

- European Union AI Act
- Council of Europe Framework Convention on AI
- UNESCO Recommendation on the Ethics of AI
- UN High-Level Advisory Body on AI and Global Digital Compact

These instruments demonstrate growing recognition that AI governance must be both principled and practically implementable. Yet none of them is specifically designed to address the full spectrum of security-related risks posed by AI or to serve as a comprehensive peace-oriented framework for algorithmic warfare and cognitive manipulation.

5. Pillars of Digital Jus Pacis

5.1. Pillar 1: Lawful Design – Human Oversight and Proportionality

The first pillar of *digital jus pacis* is lawful design: embedding legal and ethical constraints directly into AI systems used in defence and security. This goes beyond ex post review and calls for ex ante alignment of technical architectures with international law and human rights standards (Viveros Alvarez, 2024). An approach, which reframes the regulation of military and security-related AI from a predominantly logistical or international relations challenge into a question of global governance and acceptable state behaviour in the development and use of AI-enabled capabilities.

Key components include:

- **Meaningful human control.** AI systems involved in the use of force must be designed so that human operators can understand, scrutinise and override machine outputs. This entails user-centred interface design, decision-support that explains underlying reasoning, and operational doctrines that preserve human authority over critical choices (NIST, 2023). With a leaning towards Human-in-the-Loop (HITL) approaches compared to Human-on-the-Loop (HOTL) and Human-over-the-Loop (HOOTL) approaches. The key difference lies in the level and frequency of human involvement, ranging from constant collaboration (HITL) to distant supervision (HOOTL).

- **Proportionality and distinction by design.** Systems should incorporate constraints and safeguards that reflect legal obligations—for instance, conservative thresholds for target confirmation, multi-sensor cross-checking, and conservative defaults when uncertainty is high.
- **Explainability and transparency.** Black-box models may be incompatible with contexts where legal accountability requires traceability of decisions. Where opaque models are used, additional auditing layers and post-hoc explanations may be necessary (Smith & Crampton, 2024).
- **Fail-safe mechanisms and kill-switches.** War algorithms should include robust mechanisms for safe shutdown, especially when anomalous behaviour is detected or communication is lost.

By designing systems with legal and ethical constraints in mind, states can reduce the risk that AI deployments will inadvertently violate IHL, human rights, or emerging *jus ante bellum* norms.

5.2. Pillar 2: Cooperative Governance – Regional and Global Alignment

The second pillar emphasises cooperative governance and information exchange. Given that AI supply chains, data flows and security risks are transnational, no state can achieve *digital jus pacis* in isolation (Tréhu & Ricart, 2024; Global Partnership for Sustainable Development Data, 2025).

This pillar has four main elements:

1. **Global multilateral instruments.** A future AI Peace Compact could build on existing initiatives by codifying principles for responsible military AI, algorithmic transparency, and restrictions on AI in nuclear command and control.
2. **Regional frameworks and model laws.** Regional organisations can contextualise global principles by developing model legislation and guidelines tailored to specific legal traditions, threat environments and levels of capacity (ECLAC, 2024).
3. **Information exchange and transparency mechanisms.** Effective cooperation requires trusted channels for sharing information about AI incidents, vulnerabilities, deployment practices and best practices.
4. **Specialised institutions and monitoring.** Dedicated bodies, such as an international observatory on military AI or a multilateral AI safety council, could coordinate data collection, conduct independent assessments and support verification.

Cooperative governance thus centres on building a networked architecture of norms, institutions, and information flows that collectively foster restraint and reduce the risk of AI-driven conflict.

5.3. Pillar 3: Moral Restraint – Digital Humanitarian Ethics

The third pillar emphasises moral restraint by integrating human rights, intergenerational equity, environmental sustainability, and cultural pluralism into AI security governance.

- **Human rights integration.** Many scholars argue that human rights norms provide a robust ethical foundation for AI governance, particularly in terms of dignity, equality, and ensuring accountability (Jones, 2023). Factors that are already at the forefront of discussion on ethical design, especially in public governmental forums.
- **Intergenerational equity.** Decisions about AI systems, especially in nuclear, cyber and cognitive domains, can have long-term implications for future generations.
- **Environmental sustainability.** AI training and deployment can carry high environmental costs, including energy consumption and resource utilisation.
- **Cultural pluralism and openness.** Debates about open-source AI and data sharing must consider the risk of exacerbating digital divides and reinforcing dominant cultural narratives.

Moral restraint thus anchors *digital jus pacis* in a broader ethical horizon, recognising that peace in the AI era is not merely the absence of war but the presence of just, sustainable and inclusive digital orders.

6. Conclusion

AI has ushered in a new era of algorithmic warfare, cognitive manipulation and data-driven security practices. These developments strain existing legal frameworks and expose gaps in accountability, transparency and restraint. Nevertheless, they also offer an opportunity: to rethink how law, technology and ethics interact in the preservation of peace. D*igital jus pacis*, grounded in lawful design, cooperative governance and moral restraint,

can provide a valuable framework for addressing AI's security implications. This concept connects classical doctrines of *jus ad bellum* and *jus in bello* with emerging ideas of *jus ante bellum* and contemporary debates on AI ethics and governance.

To move from concept to practice, states and international organisations must deepen cooperation and information exchange, align regional and global instruments, support capacity-building in the Global South, and design AI systems that are legally and ethically constrained by default.

Literature

1. Barsade, I., & Horowitz, M. C. (2018, August 16). *Artificial intelligence beyond the superpowers*. *Bulletin of the Atomic Scientists*. https://thebulletin.org/2018/08/the-ai-arms-race-and-the-rest-of-the-world/
2. Bode, I., & Bhila, I. (2024, September 3). *The problem of algorithmic bias in AI-based military decision-support systems*. International Committee of the Red Cross – Law and Policy Blog. https://blogs.icrc.org/law-and-policy/2024/09/03/the-problem-of-algorithmic-bias-in-ai-based-military-decision-support-systems/
3. Dookeran, W., & Byng, M. (2025). Geopolitical realignment in the twenty-first century: A case for Trinidad and Tobago's strategic shift from non-alignment to multi-alignment. *Horizons: Journal of International Relations and Sustainable Development*, 30, 262–272. https://www.jstor.org/stable/48829698
4. Erai Turkey. (2025). *How AI in Turkey's industrial revolution is driving innovation and growth*. https://eraiturkey.com/2024/08/ai-in-turkeys-industrial-revolution/
5. Global Partnership for Sustainable Development Data. (2025). *A step in the right direction: UN establishes new mechanisms to advance global AI governance*. https://www.data4sdgs.org/news/step-right-direction-un-establishes-new-mechanisms-advance-global-ai-governance
6. Jones, K. (2023). *Human rights should be at the heart of AI and technology governance*. Carnegie Council for Ethics in International Affairs. https://www.carnegiecouncil.org/media/article/human-rights-ai-technology-governance
7. Lappin, Y. (2017). *Artificial intelligence beyond the superpowers*. *Bulletin of the Atomic Scientists*. https://thebulletin.org/2018/08/the-ai-arms-race-and-the-rest-of-the-world/
8. Nishimoto, J. (2025). Artificial intelligence and nuclear weapons: A critical assessment of risks and benefits. *Texas National Security Review*, 8(3). https://tnsr.org/2025/06/artificial-intelligence-and-nuclear-weapons-a-commonsense-approach-to-understanding-costs-and-benefits/
9. Ratska, M., & Bitzinger, R. A. (2023). *The AI wave in defence innovation: Assessing military artificial intelligence strategies*. Routledge.
10. Smith, B., & Crampton, N. (2024). *Global governance: Goals and lessons for AI*. Microsoft On the Issues Blog. https://blogs.microsoft.com/on-the-issues/2024/09/23/global-governance-goals-and-lessons-for-ai/
11. Smith, T. (2025a). *Cyber crisis management in the AI era: Confronting disinformation and hybrid threats* (EU CyberNet Expert Series No. 5). https://www.eucybernet.eu/wp-content/uploads/2025/10/eu-cybernet-expert-blog-series-smith-no5-2025.pdf
12. Smith, T. (2025b). Just war theory in the cyber age: Ethical implications for modern-day security. *SPOTLIGHT on Crime and Public Safety*, 5(2), 4.
13. Tréhu, J., Ricart, R. J., & German Marshall Fund of the United States. (2024). *Global AI governance: Key steps for transatlantic cooperation*. https://www.gmfus.org/news/global-ai-governance-key-steps-transatlantic-cooperation
14. United Nations. (2024). *Global Digital Compact*. https://www.un.org/techenvoy/global-digital-compact
15. United Nations High-Level Advisory Body on AI. (2024). *Governing AI for humanity: Final report*. https://www.un.org/sites/un2.un.org/files/governing_ai_for_humanity_final_report_es.pdf
16. Viveros Alvarez, J. (2024, September 4). *The risks and inefficiencies of AI-based military targeting*. International Committee of the Red Cross – Law and Policy Blog. https://blogs.icrc.org/law-and-policy/2024/09/04/risks-inefficiencies-ai-military-targeting