EDITORIAL PREFACE: AI ENABLED WEOPANS AND INTERNATIONAL LAW

Dear Readers

We are proud to present to you the 21st issue of the *Cyberpolitik Journal*. It is a great honour for all of us to continue our journey that we started nine years ago without interruption. As the digital world grows every day and every second, new developments and new technologies emerge, we are trying to read and understand this domain within our limitations.

In an era dominated by the omnipresence of technology and interconnected digital ecosystems, the role of artificial intelligence cannot be overstated. The articles featured in the 21st issue of the *Cyberpolitik Journal* bring forth a compelling narrative, shedding light on diverse facets of cyber landscapes, from ethical considerations and human rights to human rights, from cybersecurity and data protection in a digitally enriched environment.

In contemporary international law, few questions carry as much moral weight as the one addressed in this debate: Can the decision to end a human life be delegated to a machine? In less than a decade, lethal autonomous weapon systems, capable of selecting and striking targets without human intervention once activated, have moved from speculative fiction to operational reality. We see munitions and increasingly autonomous unmanned aerial vehicles (UAVs) roaming battlefields. These are becoming increasingly attractive tools for major powers and developing countries. The most influential factor in the development of these tools is artificial intelligence. Major powers have begun to delegate critical functions to systems that are no longer dependent on human hands. Many states globally, primarily the US and China, are making significant investments in these weapons. International law, as is often the case, is lagging behind in managing this dangerous technology.

The legal starting point of the issue is deceptively simple. International humanitarian law is applicable to any weapon, no matter how new. However, its fundamental principles are based on human judgment, generally on distinction, proportionality, and precaution. Distinguishing a combatant from a rifle-wielding farmer, or recognizing a wounded or surrendered combatant as a non-combatant, is rarely a matter of pattern recognition. It is a matter of context, and context is one of the things machine perception handles worst. Proportionality requires something even more delicate: comparing civilian life to military advantage under conditions

no programmer can fully predict. Whether such judgments can be codified into software, or at least pre-executed by humans, divides the field by tightly limiting the targets, geography, and duration of a system. It provides a basis for international procedures that compel states to review the legality of new weapons. But this basis is designed for predictable technologies rather than learning systems whose behavior can be uncertain even to their designers.

Underlying the doctrinal questions lies a structural question: who is accountable, or what is accountability? International criminal law presupposes a human perpetrator who has intent, makes a decision, and can be held responsible for what happens afterward. However, a machine has no intent and cannot be judged. Any military operation may have acted reasonably based on the available information. However, the programmer is far from harm in terms of time and space. Robert Sparrow's warning about the **"liability gap"** raises the concern that when an algorithm makes a mistake, no one can be held responsible for deaths. Others argue that the law of command responsibility and state responsibility could be adapted to close this gap, meaning that a commander who unleashes an unpredictable weapon into a crowded area is guilty in the oldest sense of the word. The reader will decide which view is more convincing. What neither side disputes is that the application architecture built since Nuremberg is strained under the weight of distributed algorithmic action.

The ethical debate is equally polarized. For opponents, the objection is deontological and absolute. To be killed by an algorithm means to be reduced to a data point, to be deprived of human dignity, a life weighed on doubt, hesitation, and mercy. For supporters, especially those associated with Ronald Arkin, the question is empirical rather than categorical. Machines don't panic, seek revenge, or fire out of fear, and if they can save more civilians than soldiers under stress, refusing to deploy them would be a moral failure in itself. Between these poles, the concept of "**meaningful human control**" has emerged as the common language of diplomacy. It is attractive in principle, vague in specification, and clouded by automation bias that is, the tendency for humans to submit to the machine they are tasked with controlling.

The diplomatic landscape reflects this unresolved tension. Decades of negotiations under the Conventional Arms Treaty have produced guiding principles, not binding rules. This has been hampered by the need for compromise and resistance from major military powers. Consequently, momentum has shifted to the UN General Assembly. The General Assembly's recent resolutions have been adopted by an overwhelming majority, requesting the Secretary-

General to enact a binding regulation. This regulation would ban autonomous weapons operating without human control and tightly regulate the rest. Whether these efforts will translate into treaty law, or whether state practices will quietly normalise autonomy, much like the once-normalised armed drones, will be the defining question of the coming years.

Contents of the New Issue

As artificial intelligence moves from the margins of technological debate to the very centre of security, diplomacy, and governance, the questions it raises grow more urgent and more complex. Algorithms now shape not only how states defend their networks but also how societies perceive truth, how power is distributed across the international system, and how individuals experience security in their daily lives. The contributions to this issue of Cyberpolitik Journal take up these questions from a variety of disciplinary and regional perspectives, examining the intersection of artificial intelligence, cybersecurity, and international politics through articles, opinion pieces, and reviews.

The first article of the new issue, The *Gendered Dimensions of AI-Driven Security*, Muskan Moazzam and Haris Bilal Malik bring a critical and often overlooked perspective to debates on artificial intelligence and security. The study explores how AI-driven security technologies from surveillance systems to automated decision-making tools are neither designed nor deployed in a gender-neutral manner. Drawing attention to algorithmic bias, unequal patterns of vulnerability, and the underrepresentation of women in the design of security technologies, the article argues that a genuinely comprehensive approach to AI security must incorporate gender analysis. In doing so, it enriches the literature by connecting feminist security studies with contemporary debates on emerging technologies

In the second article, *Siber Güvenlik Tehdidi Olarak Dezenformasyon: Dijital Güvenlik ve Diplomasi Açısından Etkileri* by Hüma Gül Çakır, addresses disinformation as a genuine cybersecurity threat rather than a mere communication problem. The article examines how deliberately manufactured and rapidly disseminated false information undermines digital security, erodes public trust, and complicates the conduct of diplomacy between states. By situating disinformation within the broader architecture of digital security, the author demonstrates that countering it requires not only technical defenses but also coordinated diplomatic responses, and offers a framework for understanding how states can protect both their information environments and their foreign policy credibility in an era of weaponized narratives.

The third article, *Lebanon's Strategic Position in the Age of AI-Driven Defense and Cybersecurity* by Sarkis Karaguezian**,** turns the reader's attention to the regional level. The study assesses how a small state situated in one of the world's most volatile regions navigates the accelerating competition over AI-enabled defense capabilities and cybersecurity infrastructure. Analysing Lebanon's geopolitical constraints, institutional capacities, and external dependencies, the article discusses both the risks that AI-driven military technologies pose for the country and the opportunities that strategic adaptation may offer. It thereby contributes a valuable case study to the growing literature on small states and emerging technologies.

The last article, *Gıda Rejimi ve Dijitalleşme: Teknolojik Örgütlenmeye Yapısal Bir Yaklaşım* by Salim Bülent Yüksel, addresses a significant gap in the existing literature by re-examining the relationship between digital technologies and food regimes. The study positions digitalization not as an external factor, but as a structural dynamic shaping food production and circulation through data, platforms, and algorithms.

The first opinion piece of the issue, *Cyber Security in the Age of Artificial Intelligence* by Mehmet Emin Erendor, offers a panoramic reflection on how artificial intelligence is transforming the fundamental logic of cybersecurity. The author considers the dual-use character of AI as both a powerful defensive instrument and an unprecedented tool in the hands of malicious actors and reflects on what this duality means for states, institutions, and individuals alike.

In the second commentary, *Digital World-System Hierarchies and AI-Driven Security Competition*, Fahad Nabel presents a powerful and original piece that blends world-systems theory with the realities of contemporary technological rivalry. The author maps the emerging hierarchy of core, semi-peripheral, and peripheral actors in the digital domain and argues that competition over artificial intelligence is reproducing – and in some respects deepening – the structural inequalities of the international system. The commentary offers the reader a crucial perspective on how AI-driven security competition is reshaping global power relations.

The third opinion piece, *Geleneksel İstihbaratın Sınırında Siber Operasyonlar: Mossad'ın Hizbullah'a Yönelik Çağrı Cihazı Saldırısı* by Necati Yıldız examines one of the most striking intelligence operations of recent years. Taking the pager attack attributed to Mossad against

Hezbollah as its case, the commentary discusses how cyber capabilities, supply-chain infiltration, and traditional intelligence tradecraft have converged, blurring the boundaries between espionage, sabotage, and armed conflict. The piece raises important legal and ethical questions about the future of covert operations at the intersection of the physical and digital worlds.

Finally, two reviews provide valuable insights into the current literature. Müfide Onur reviews *Cyber Security in the Age of Artificial Intelligence and Autonomous Weapons*, a volume that explores how autonomous systems and machine intelligence are redefining the threat landscape and the requirements of national defense. In the second review, Saliha Nur Köşger evaluates *The Ethics of Information*, guiding the reader through its philosophical treatment of information as a moral concern and highlighting its relevance for anyone seeking a normative foundation for debates on the digital age.

In summary, the articles, commentaries, and reviews in this issue contribute to a better understanding of the opportunities and risks that artificial intelligence brings to the domains of security, diplomacy, and international order. These contents, prepared with academic depth, aim to open doors to interdisciplinary thought and new areas of discussion. We hope they inspire our readers and open new horizons.

Kamil TARHAN, Ph.D

Issue Editör