WAR AND PEACE IN THE 21ST CENTURY

3RD EDITION

NEW TECHNOLOGIES AND INTERNATIONAL LAW

04 October 2024

ABSTRACTS

Edited by Zsuzsanna CSAPÓ

Venue

Ludovika Campus

Hungary – 1083 Budapest, 2 Ludovika tér

Organizers

Department of International Law at the Faculty of Public Governance and International Studies at Ludovika University of Public Service, Budapest, Hungary

Tamás CSABA

Zsuzsanna CSAPÓ

András HÁRS

Noémi NAGY

Melinda SZAPPANYOS

Balázs VIZI

Réka VARGA (Dean, Head of the Department)

Theme of the conference

International law is often criticized as both subservient to political will and lacking options for enforcement when it comes to unwilling states. From the frontiers of humanity brought by new technologies and renewed vigour in space exploration, to the use of artificial intelligence in armed conflict as well as its ramifications for human rights, international law faces significant challenges questioning its strength, validity and legitimacy. The theme of this year's conference aims to discuss these myths by delving into areas of public international law in which technological development is shifting traditional boundaries and forces a re-evaluation of classic concepts.

NATIONAL UNIVERSITY
OF PUBLIC SERVICE
LUDOVIKA

FACULTY OF PUBLIC GOVERNANCE AND
INTERNATIONAL STUDIES
DEPARTMENT OF INTERNATIONAL LAW

SESSION NO.1.

International Regulation of Emerging Technologies and of Space

NATIONAL UNIVERSITY OF PUBLIC SERVICE
LUDOVIKA

FACULTY OF PUBLIC GOVERNANCE AND INTERNATIONAL STUDIES
DEPARTMENT OF INTERNATIONAL LAW

Rachita AGRAWAL

Research Fellow – Guru Gobind Singh Indraprastha University, Delhi, India

ROLE AND RELEVANCE OF SPACE TECHNOLOGY IN WARFARE

The warfare situations have always been asymmetric. With the exploration and utilization of outer space, the nations are devising unique strategic advantages. Nations equipped with infrastructure, technical capabilities and resources are able to formulate military plans, actions and defense system, ahead of time. The non-space faring nations are devoid of benefits that could be derived from space-based insights. The differences in space technology capabilities, approach and policy exposes vulnerabilities among nations threatening the global peace and security, just as it was seen during World War II (atomic bombing in Japan). The positioning of objects in new frontier, which is still not comprehensively govern promotes extension of geopolitical competition beyond Earth. The presentation examines role and utility of space technology in the warfare, the legal implications and challenges posed for international stability.

KEYWORDS: warfare, peace, space technology, global stability

Mónika GANCZER

Associate Professor – Széchenyi István University Deák Ferenc Faculty of Law and Political Sciences Department of International and European Law, Győr, Hungary

Research Fellow – HUN-REN Centre for Social Sciences Institute for Legal Studies, Budapest, Hungary

External Researcher – Ludovika University of Public Service Institute of Space Law and Policy, Budapest, Hungary

KNOW YOUR ENEMY: SPACE ACTIVITIES OF NON-GOVERNMENTAL ENTITIES IN INTERNATIONAL ARMED CONFLICTS

In recent years, space activities have been increasingly carried out by non-governmental entities. In 2023, non-governmental entities, rather than states, accounted for more than three quarters of the $546 billion annual space economy. Furthermore, the involvement of non-governmental entities in space activities is also on the rise in the context of international armed conflicts. States bear international responsibility for national activities carried on by non-governmental entities under Article VI of the 1967 Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies. The interpretation of this Article, in particular the expressions of national activities, appropriate state, non-governmental entities is also crucial in international armed conflicts to identify the state behind the space activity. Furthermore, the potential for states to supervise these activities also requires analysis in order to regulate and restrict these private activities on the part of the state.

KEYWORDS: private space activities, non-governmental entities, appropriate state, national activities, responsibility

NATIONAL UNIVERSITY OF PUBLIC SERVICE
LUDOVIKA

FACULTY OF PUBLIC GOVERNANCE AND INTERNATIONAL STUDIES
DEPARTMENT OF INTERNATIONAL LAW

Mátyás KISS

PhD Student – University of Pécs Faculty of Law, Hungary

THE SOVEREIGNTY OF STATES IN CYBERSPACE

The principle of sovereignty is one of the cornerstone norms of modern international law. The precise content and meaning of this fundamental principle have changed significantly in historical and political contexts, often sparking intense debates. Today, one of the most critical questions regarding sovereignty is how this principle can be applied in cyberspace. In recent years, the number of hostile cyber operations between states has increased dramatically. By the beginning of the 2020s, various international organizations had already recorded more than a hundred incidents annually.

In my research, I primarily seek to answer the question of which cyber operations may violate the sovereignty of a territorial state. In 2020, actors likely linked to Russia breached the systems of SolarWinds, which may have been the largest cyberattack in history. SolarWinds is a significant software company in the US that provides system management tools for network and infrastructure monitoring, as well as other technical services, to hundreds of thousands of organizations worldwide, including the United States government.

If the SolarWinds attack was carried out by a state – in this case, Russia – it could be considered a violation of state sovereignty. Even though the attack did not cause any deaths or physical damage, the targeted infrastructure had to be reinstalled to perform its intended purpose, which is a form of losing functionality.

My opinion is based on the framework outlined in the Tallinn Manual, which is one of the most significant private codification efforts regarding the relationship between cyberspace and international law. In the absence of relevant international treaties, such works, along with expanding state practice, play a crucial role.

KEYWORDS: Tallinn Manual, state practice, cyber operations, sovereignty, international law

NATIONAL UNIVERSITY OF PUBLIC SERVICE
LUDOVIKA

FACULTY OF PUBLIC GOVERNANCE AND INTERNATIONAL STUDIES
DEPARTMENT OF INTERNATIONAL LAW

Anna Dóra KOVÁCS

PhD Student – Ludovika University of Public Service, Budapest, Hungary

OPPORTUNITIES FOR THE ETHICAL REGULATION OF ARTIFICIAL INTELLIGENCE THROUGH A COMPARISON OF LEGISLATION IN THE EUROPEAN UNION, UNITED STATES OF AMERICA AND CHINA

The study aims to provide a comparative analysis of the ethical regulation of artificial intelligence (AI) based on the relevant legislature of the European Union, the United States of America, and China. The European Union's regulation deals with transparency, responsibility, and human control issues regarding AI. The American regulation employs a sector-specific approach, whereas China incorporates national, regional, and local regulations into its legislative framework.

Both similarities and differences can be observed regarding conceptual definitions and ethical principles. Whereas the European Union and China adopt a more precautionary, even stricter approach to the topic, the United States prefers a more lenient, market-oriented stance. Underlying political, economic, and cultural factors also influence individual legislations to a notable degree.

Challenges for the regulations include the fast pace of change in AI technology itself, as well as establishing a balance between individual rights, economic growth, and governmental oversight. Opportunities and limitations for cooperation are also discussed in comparing the three actors.

Overall, regulating AI is an intricate task requiring both ethical and technical expertise, as well as cooperation between stakeholders, to appropriately address issues surrounding the benefits and risks stemming from the technology.

Gábor SULYOK

Full Professor – Széchenyi István University Deák Ferenc Faculty of Law and Political Sciences Department of International and European Law, Győr, Hungary

SPACE THREATS AND THE UN SECURITY COUNCIL

The presentation will analyse the functions and powers of the United Nations Security Council in the context of space threats. The topic had initially received little scholarly attention, but recent events have placed the issue of space threats on the Security Council's agenda. For the purposes of the presentation, the concept of space threats is understood broadly to include any conduct involving space objects and/or outer space that may warrant the attention of the Security Council. Following the examination of the Security Council's inventory in addressing space threats, the presentation will also assess the feasibility of preventive or enforcement action in the prevailing organizational and international environment.

KEYWORDS: UN Security Council, peace and security, outer space

NATIONAL UNIVERSITY OF PUBLIC SERVICE
LUDOVIKA

FACULTY OF PUBLIC GOVERNANCE AND INTERNATIONAL STUDIES
DEPARTMENT OF INTERNATIONAL LAW

Zoltán TURBÉK

Deputy Permanent Representative of Hungary, Geneva – Permanent Mission of Hungary to the United Nations and other International Organizations in Geneva, Switzerland

Former Co-Chair – Council of Europe's CAHAI Policy Development Group

Member – Council of Europe's Committee on Artificial Intelligence (CAI)

Head of delegation during the negotiations of the UNESCO Recommendation on the Ethics of AI

INTERNATIONAL REGULATION OF THE USE OF ARTIFICIAL INTELLIGENCE SYSTEMS – NEW REGULATORY INITIATIVES

As the potential and risks of Artificial Intelligence (AI) are becoming increasingly evident, the number of initiatives by international organizations aimed at regulating the use of this technology is also growing. In addition to the new regulatory attempts, there are also existing normative instruments that could be considered already applicable to the use of AI systems.

The presentation will identify the main features of the most recent regulatory initiatives (e.g. by UNESCO, OECD, EU, Council of Europe, ITU). The presenter will then study the impact of these parallel processes for normative development. Will these instruments contradict each other and result in conflicting rights and obligations, or they could serve as complementary, mutually supportive pieces of a larger normative framework? Will these processes lead to a fragmented international legal landscape, or there was still room to harmonize the developing legal frameworks and determine common norms and principles in this new field of law that we may call emerging "international AI law". The presenter will also explore if there was a need for the development of a new AI treaty under the auspices of the United Nations.

KEYWORDS: AI systems, new regulatory initiatives, soft law, hard law, AI treaty, technical standards, fragmentation, complementarity, emerging international AI law

NATIONAL UNIVERSITY
OF PUBLIC SERVICE
LUDOVIKA

FACULTY OF PUBLIC GOVERNANCE AND
INTERNATIONAL STUDIES
DEPARTMENT OF INTERNATIONAL LAW

SESSION NO.2.

International Humanitarian Law and International Criminal Law Implications of Emerging Technologies

NATIONAL UNIVERSITY OF PUBLIC SERVICE
LUDOVIKA

FACULTY OF PUBLIC GOVERNANCE AND INTERNATIONAL STUDIES
DEPARTMENT OF INTERNATIONAL LAW

Muhammad Abdullah FAZI

Lecturer – Monash University, Malaysia

MITIGATING BIASED AI ALGORITHMS: THE RISKS OF REPORTING WAR CRIMES ON SOCIAL MEDIA PLATFORMS

The presentation examines the challenges of preserving evidence of war crimes documented on social media platforms. Tech companies such as Meta and YouTube use artificial intelligence (AI) to quickly remove content, sometimes without archiving it, including evidence of potential war crimes. As evidenced by the conflicts in Syria and Ukraine, this has resulted in the loss of vital documentation. The cautious moderation policies of the industry meant to safeguard users, unintentionally obstruct justice by deleting evidence that may support legal prosecutions and protect civilians in warfare. To highlight the bias in moderation policies of social media platforms that reflect in respective algorithms, this study examines particular case studies of modern conflict reporting on social media suggesting a review of existing frameworks and implementation of effective mechanisms that strike a balance between content moderation and the preservation of vital war crime evidence under the ambit of international humanitarian law.

KEYWORDS: AI, IHL, war crimes, social media

NATIONAL UNIVERSITY OF PUBLIC SERVICE
LUDOVIKA

FACULTY OF PUBLIC GOVERNANCE AND INTERNATIONAL STUDIES
DEPARTMENT OF INTERNATIONAL LAW

Krzysztof KAZMIERCZAK

Lecturer – University of Lodz, Poland

DOES A SMARTPHONE MAKE A SOLDIER? SMART DEVICES AND PARTICIPATION IN HOSTILITIES UNDER INTERNATIONAL HUMANITARIAN LAW

Developments of the last two decades in the market of smart or mobile phones resulted in a situation where almost every adult person carries with them at all times a digital camera with an ability to transmit image to any other place in the world. Potential military applications of such capability are significant. Ukrainian-Russian conflict did see development of dedicated apps, such as Ukrainian ePPO, which can be used to detect air targets, identify them and transmit data on them to air defense. This application has been credited as allowing successful engagement of multiple air targets.

Such activities – as those which can be carried out using ePPO – are effectively direct participation in hostilities which temporarily suspends the protection afforded to under the Additional Protocol II (AP II) to the Geneva Conventions (1977). ePPO application alone has been downloaded by well over 180.000 people, but does not constitute a sole way in which civilian may be understood to participate in hostilities. Just making and sharing photos of military positions could raise questions concerning such direct participation.

The presentation will answer two questions: What are the challenges to framework of ius in bello from the usage of smart devices and when can we talk about direct participation in hostilities? What duties involved parties – civilians, soldiers, app developers and distributors, governments – have, related to the usage of smart devices and how are currently such duties fulfilled?

NATIONAL UNIVERSITY OF PUBLIC SERVICE
LUDOVIKA

FACULTY OF PUBLIC GOVERNANCE AND INTERNATIONAL STUDIES
DEPARTMENT OF INTERNATIONAL LAW

Bence KIS KELEMEN

Senior Lecturer – University of Pécs Faculty of Law, Hungary

HACKING AS DIRECT PARTICIPATION IN HOSTILITIES

The Russia-Ukraine international armed conflict has highlighted how crucial it is to understand military operations taking place in cyberspace and be aware of their immediate consequences for individuals. In many instances, civilian hackers have played a role in the aforementioned armed conflict by executing various cyber operations.

The purpose of the presentation is to illustrate under what circumstances the activities of civilian hackers may be considered direct participation in hostilities, resulting in the targetability of such individuals. The presentation will show, on the one hand, that only a handful of cyber operations will be capable of reaching the necessary threshold of harm (e.g. attacks as defined under international humanitarian law), and on the other hand, that targetability due to direct participation can lead to the deployment of cyber and conventional weapons alike against the individual in question.

The presenter will also deal with the temporal aspect of targetability and show that civilian hackers participating in the hostilities can be targeted during the implementation of and immediate preparation for cyber operations or – if they assume a function related to combat in an armed group – until the termination of their involvement in the organization.

The presentation also delves into the related state practice, shedding light on how members of the international community currently contemplate this issue.

KEYWORDS: cyber operations, direct participation in hostilities, international humanitarian law, targetability, continuous combat function

NATIONAL UNIVERSITY OF PUBLIC SERVICE
LUDOVIKA

FACULTY OF PUBLIC GOVERNANCE AND INTERNATIONAL STUDIES
DEPARTMENT OF INTERNATIONAL LAW

Tamer MORRIS

Senior Lecturer – University of Sydney, Australia

INFORMATION WARFARE AND THE PROTECTION OF CIVILIANS IN ARMED CONFLICT

Disinformation attacks have become a common tool within military strategy. Information warfare is still generally not considered to fall within the scope of international humanitarian law (IHL). In analyzing IHL, the principle of the protection of civilians must be the lens to interpret its provisions. Unlike ruses of war and propaganda, disinformation operations are intending to inflict harm on the populace, and therefore, cannot be unregulated. The concept of an 'attack' should be reconceptualized when the resulting effect of the military operation is the harm of civilians. Moreover, as civilians are never to be a target of a military operation, any disinformation operation intending harm on civilians would be a violation of a party's obligation under IHL. Even if no harm is actualized a disinformation operation would violate a party's obligation if the intended target were civilians.

NATIONAL UNIVERSITY OF PUBLIC SERVICE
LUDOVIKA

FACULTY OF PUBLIC GOVERNANCE AND INTERNATIONAL STUDIES
DEPARTMENT OF INTERNATIONAL LAW

Maria VARAKI

Lecturer – King's College, London, United Kingdom

AI "INDUCED" WAR AND PEACE?

During the 2022 Venice Biennale of Art, a robot Ai-Da, had her first solo exhibition in the Giardini gardens titled "Leaping into the Metaverse". The exhibition was inspired by Dante's Divine Comedy, questioning also the dark side of AI; in other words how much of AI do we want and we can accept?

From one side new technologies facilitate faster proceedings and accelerate decision making. From the other side there is a series of ethical, legal and policy questions about the limits of non-human judgment, the necessity or not of a "new" right not to be subjected to automated decision making and the responsibility of those who design the relevant algorithms. Having said that, it is also important not to idealize human rationality. Several human fellows do not indicate common sense and rational judgment. Additionally, human judgments are influenced by personal biases and prejudices.

Within this context, the presentation aims to explore first the use of AI in armed conflicts and in particular, in the identification of military targets and second AI's utilization in mediation processes. The key questions to be addressed are as follows; is there a legitimate risk of dehumanization sensibility in war and peace? And if so, where do we need human judgment? Finally, what is the ideal formula to avoid dehumanization? The framework of human rights law, a different regulatory method, or an idiosyncratic sensibility of responsibility?