esil sedi
EUROPEAN SOCIETY OF INTERNATIONAL LAW

FACULTY OF LAW
Charles University

New Technologies in International Law

ABSTRACT VOLUME

TABLE OF CONTENTS

1 BAKOŠOVÁ LUCIA - *THE RIGHT TO CLEAN, HEALTHY AND SUSTAINABLE ENVIRONMENT IN ARTIFICIAL INTELLIGENCE ERA*

The current period is also often referred to as the period of industrial revolution 4.0, where one of the main roles is played by the development and use of artificial intelligence across industries. In general, artificial intelligence is mostly regulated by States (although only several States worldwide adopted legal regulation on development, manufacturing or use of artificial intelligence) active in introducing new technologies into everyday life. On a wider level, the European Union adopted several documents on artificial intelligence, most notably the draft of the so called "Artificial Intelligence Act". Due to the special features of the artificial intelligence, such as inexplicability of its results, potential threat to human rights, accountability etc., special legal regulation that reflects the abovementioned is necessary. It is widely accepted that the development of artificial intelligence and its use must be in accordance with existing international and domestic norms. The emphasis is mainly on compliance with the norms of international human rights law. Since the international human rights law is still evolving, the existing catalogue of human rights is expanding to include rights that are closely linked to sustainable development and the environment. Although discussions about the existence of the right to a clean, healthy and sustainable environment last for several years, only in 2022 the UN General Assembly adopted resolution no. 76/300, which recognizes the right to a clean, healthy and sustainable environment as human right. The aim of the paper is to answer the main question: "Do the adopted or draft international norms regulating the use of artificial intelligence reflect on the right to clean, healthy and sustainable environment? Such aim will be fulfilled through analysis of international legally binding, as well as non-binding documents on artificial intelligence adopted by international organizations (such as UN, EU or OECD) and non-state actors. The author will also focus on the right to clean, healthy and sustainable environment, its content and international recognition.

2 BIRD CHARLES ROSS - *A CHANGING VIEW OF NON-APPROPRIATION OF SPACE RESOURCES*

In order for the space resources industry to grow, some type of legal certainly must be established to ease the minds of those willing to risk venturing into this arena. Despite the international discussions in the framework of the UN COPUOS, there is no UN treaty or global convention on the horizon. To make some reasonable predictions for the future, one can often look to the past. In 1945, US president Harry Truman proclaimed that the US had sovereign control of the continental shelf. This included the right to resources found there and enacted domestic law allowing private persons to acquire ownership in any resources extracted. At the time this went against the custom that resources within a continental shelf were a global common and could not be appropriated by any state. However, a global outcry was not heard. In fact, other states began to enact similar domestic laws. This finally culminated with the 1967 North Sea Continental Shelf Cases in front of the ICJ. In those cases, the Court found that states had a right to the resources found on their continental shelves, in part because rather than contest the decision of the US, they chose to acquiesce to it and follow suit. The impetus for this change, among others, was the need to control coastal waters and prevent overfishing. This protection then led to an explosion of resource development from the continental shelf that would not have been possible without a legal regime that provided clarity and the ability to develop. A parallel can be drawn to the current legal state of resources found in space, specifically those found on or in celestial bodies. Currently, some hold a view that the Article II OST prohibits appropriation to those resources. However, just like Truman's announcement, in 2015, US President Barack Obama signed into law the Commercial Space Launch Competitiveness Act which allows US private entities to acquire ownership in any space resources they recover. This time however, the motivation for this change has been the rapid development of technology that will make it possible to extract and utilize these resources as well as the entry of private actors into the space arena. Multiple states have followed suit and enacted their own domestic legislation allowing the same, such as Luxemburg in 2017, the UAE in 2019, and Japan in 2021. The US Artemis Accords section on space resources states that there is no conflict with Article II OST and its view on the utilization of space resources. As of July of 2023, the Accords has 28 signatories agreeing to that concept. It would seem that the future of space resources is following the path of other formerly untouchable resources. This the author believes provides a forecast for those looking to enter into this industry and take the risks associated with it with a bit more peace of mind.

3 BYCZYNSKI MICHAL - *SECURING THE POST-PANDEMIC WORLD: WHAT IS THE CURE FOR INFODEMIA?*

The COVID-19 pandemic has fundamentally changed the way individuals live, accelerating the digital transformation of society and creating new cybersecurity challenges. As we are moving towards a post-pandemic world, it is essential to reassess cybersecurity strategies to be prepared for the emerging threat landscape.

The presentation will discuss the key cybersecurity solutions for one of the post-pandemict hreats to human rights in the world: infodemia. To address these issues, desk research will be used, focusing on relevant reports, manuals, and doctrinal proposals in the context of cybersecurity.

First, the difference between the pre-pandemic and post-pandemic world needs to be addressed. The pandemic has led to an unprecedented increase in, for example, remote work, e-Commerce, and online activity. The pandemic has led to unprecedented growth in remote work, e-commerce, and online activity, for example. The ease of information dissemination has contributed to the rapid and far-reaching spread of both accurate and inaccurate data on certain issues, which gave birth to infodemia.

Infodemia means too much information including false or misleading data in the digital environment. It causes confusion and risk-taking behaviors that can harm health. It also leads to mistrust in health authorities and undermines the public health response.

Stating that infodemia is an issue arising only during the pandemic would be false. It is a truly more complex and broad issue, closely linked to misinformation and disinformation. However, the pandemic has shown how easy false information is spread. This problem is likely to become more and more common in the post-pandemic world. The influence of misinformation and disinformation on human rights is serious, as those two may have a dramatic effect on whether and how individuals are capable of exercising their rights and freedoms (right to privacy, right to peaceful assembly and association, right to health, right to education, right to freedom of expression, prohibition of discrimination, and others).

Second, possible infodemia solutions for the post-pandemic world will be examined. The presentation will present the latest technologies, including artificial intelligence, machine learning, and blockchain, and their potential to enhance cybersecurity resilience. These technologies can analyze massive amounts of data and identify patterns or anomalies not being detectable for humans. AI and ML can improve incident response times by automating the detection and mitigation of security incidents.

To overcome infodemia it is essential to adopt a risk-based approach to cybersecurity. This approach involves identifying specific cybersecurity risks and implementing the technologies that will most effectively address those risks. It is also essential to ensure that cybersecurity technologies are developed and implemented ethically and responsibly, which often brings out the issues of balancing between efficiency and law accuracy.

To conclude, the pandemic led to new and complex cybersecurity-related human rights challenges. One of them is infodemia, which requires international actors to employ innovative and collaborative solutions to combat it effectively. This presentation will provide an opportunity to explore strategies that may be useful in this process.

4 CHOIŃSKA ZUZANNA - *PROTECTION OF PRIVACY AND NATIONAL SECURITY BY THE EUROPEAN UNION INSTITUTIONS ON THE EXAMPLE OF EUROPOL IN LIGHT OF THE DEVELOPMENT OF NEW TECHNOLOGIES*

The paper aims to analyze the issue of balance between protecting public security and human rights such as the right to protection of personal data in light of the jurisprudence of the Court of Justice of the European Union (CJEU) and the European Court of Human Rights (ECtHR). In recent years, the fight against crime and the related protection of public safety has become more difficult due to the rapid development of technological solutions and its increasing use by the criminals. Furthermore, in order to meet the new challenges, law enforcement agencies have also had to adapt the digital tools that they use or implement new ones which are, very often, deployed and provided by private companies. Thus, the questions arise whether European Union's institutions such as the European Union Agency for Law Enforcement Cooperation (Europol) should be given more competences as the execution of tasks in this area at a higher level than national could turn out as more effective and how to effectively protect citizens' privacy.

What is more, the grounds for data processing by Europol will be identified as in recent years the legal basis for its activity has been amended to establish a more precise legal framework for the protection of the right to privacy and personal data. The specific focus will be placed on the competences of the European Data Protection Supervisor (EDPS) towards the agency, and discussed on the example of the technological tools used nowadays such as software of Clearview AI - a private company providing facial recognition services. It will allow me to examine the issues regarding the use of private software by law enforcement and how technological changes have impacted the scope of the processed data within years.

The analysis will be used to observe to what extent the EU principles formulated by the CJEU are implemented by Europol in regard to the changes and challenges that come with the rapid technological developments. In the second instance it will allow me to identify and propose possible changes in new safeguards that could enhance the level of protection of personal data of citizens.

5 GERLE MAREK & CRHÁK ADAM - *THE LIMITS TO THE USE OF FORCE IN CYBERSPACE: THE TALLINN MANUAL IN PERSPECTIVE OF THE ONGOING LEGAL DEBATE*

The advent of cyberspace has redefined the landscape of conflict and warfare, necessitating a reevaluation of traditional notions of the use of force in international law. Through a comparative analysis of the Tallinn Manual and the broader landscape of international legal frameworks, this paper emphasizes the Manual's role in shaping the discourse on self-defense, and the protection of critical infrastructure in cyberspace. It delves into the Manual's interpretations of Article 2(4) of the United Nations Charter and Article 51 concerning self-defense, elucidating the Manual's stance on applying traditional principles to a rapidly evolving digital environment.

Another indispensable basis for the study of the given topic is a set of relevant states' positions that indicate their *opinio iuris* in this pressing matter. These are the most up-to-date examples of the current discourse that hand to hand with future state practice might amalgamate and result in new customary norms of the general international law. The paper further investigates the complexities of attributing cyber activities and attacks to state actors, while acknowledging the inherent difficulties of the attribution process. The paper aims to offer insights into the current approach proposed by the Manual, propose other potential solutions, and invite further discussion.

In conclusion, this paper underscores the significance of the Tallinn Manual as a foundational document that endeavors to provide clarity and coherence amidst the complexities of the use of force in cyberspace within international law. By critically analyzing its provisions and implications, this study contributes to the ongoing dialogue surrounding the adaptation of legal norms to the challenges posed by the digital age, facilitating a more nuanced and comprehensive understanding of state behavior and responsibility in the realm of cyberspace.

6 D´EVEREUX VERONIKA -

IMPACT OF NEW TECHNOLOGIES USED AND DEVELOPED BY THE STATE OF ISRAEL ON HUMAN RIGHTS

In the year 2022 Israeli Ministry of Innovation, Science and Technology announced launching the National Artificial Intelligence (AI) plan, which is a long-term plan aimed at assisting in development and implementation of the AI in the public sector. The State of Israel strives to become one of the three leaders in the AI technologies by 2030. The use of the AI in the public sector brings several legal issues, one of them is the protection of the human rights. The AI can be used or misused in many ways in connection to the issues the State of Israel is facing on a daily basis. One of these issues is terrorism and other security threads. The AI systems can be used as a spyware which can monitor the daily activities of civilians and to collect the data about potential preparation, pursuing, supporting or least but not last financing the terrorist activities of Hamas and Palestinian Islamic Jihad. The infiltration of the terrorists among civilian inhabitants, including the civilians who live in the refugee camps is one of the common problems. Therefore, the spyware might interfere with the right to private life and from the perspective of the international law, it can be evaluated, how proportional is it in the context of the security threads Israel deals with. Another option is using autonomous or semi-autonomous weapons and drones to neutralize the terrorist and prevent them to complete the terrorist attack. The fully autonomous AI weapon systems might face challenge of distinguishing between the civilians and combatants, which is another problem due to the fact that the Palestinian terrorists do not have the status of the combatants but are rather armoured civilians using the weapons or suicide bombs to commit a crime of a terrorist attack. The semi-autonomous AI weapon systems might be less problematic in case they are operated by a human being which takes the final decision to activate the weapon and neutralise or injure the perpetrator. Therefore, it can be examined the level of protection of the human rights of the terrorists in case of use the artificial intelligence weapon systems for safety and security reasons and to prevent, stop or mitigate the terrorist attack or its range. This research will be dedicated to examining the current level of the AI technologies used by the State of Israel in connection to the sources of the international law. There will be also included the assessment of the relevant past incidents in which the State of Israel used the AI technologies.

7 PAPPA FOTO - *DIGITAL AGRICULTURE: SAFEGUARDING HUMAN RIGHTS THROUGH RESPONSIBLE RESEARCH AND INNOVATION*

Characterized as the fourth agricultural revolution, digital agriculture encompasses the use of digital technologies such as robots, drones, sensors, Internet of Things (IoT) and AI. It is being presented as a solution to population growth and the threat of climate change, namely as a way to ensure food security through increased food production. However, according to critical social sciences, power asymmetries are expected to deepen, and inequalities between farmers exacerbated. The risks that the deployment of the method of digital agriculture may engender, have been underlined by social scientists. To illustrate, a correlation between a large farm size with the adoption of digital agriculture technologies has been presented in literature, arguing that digital agriculture may progressively drive more and more small food producers out of agriculture.

Most legal literature so far has focused on data issues, concerning the use of the data collected by digital agriculture technologies. Concurrently, more and more states are introducing related policies (Ethiopia and Armenia are two examples), while the European Union in its Common Agricultural Policy (CAP) has characterized the digitalization of agriculture as a cross-cutting objective of the policy. In response to these developments, in my submission, I will be examining whether the potential impacts of digital agriculture on human rights, namely on the right to food and the right to science, could be addressed through an approach based on human rights and responsible research and innovation. I will thus be exploring the possibility of introducing measures such as participation in decision-making and human rights impact assessments in order to pre-emptively address the negative impacts that could ensue from the introduction of digital agriculture, especially for small farmers. Concludingly, I believe that an analysis of said risks, as well as an approach based on human rights obligations and responsible research and innovation is a timely response to a particularly topical issue and certainly merits discussion.

8 GAPSA MIŁOSZ - *HOW URGENT IS URGENT? CASE MANAGEMENT AND NEW TECHNOLOGIES IN PROVISIONAL MEASURES PROCEEDINGS*

Raison d'être of provisional measures is the urgent risk of irreparable prejudice that may occur before the final decision in the case. The conduct of the parties may influence the state of urgency. In *Pakistani POW* case, Pakistan attempted to postpone the provisional measures proceedings it had initiated. As a result, the Court deemed the request as not being urgent, and Judge Nagendra Singh even likened Pakistan's conduct to a withdrawal of the request itself.

Urgency affects the course of proceedings. As an exception, only the oral phase is required. The dates for oral hearing are fixed to "afford the parties an opportunity of being represented at it" (Article 74(3) of the ICJ Rules). However, on some occasions, the parties were unable to appear. In *Polish Agrarian Reform* case, Poland (respondent) requested a postponement of the oral phase, which the Court granted after initial reluctance. In *Electricity Company of Sofia and Bulgaria* case, Bulgaria (respondent) was absent due to the ongoing Second World War.

Furthermore, Article 74(1) of the ICJ Rules stipulates that provisional measures proceedings are given priority over other activities of the Court. However, the Court displays inconsistency in setting the dates for oral hearings and delivering the order. In *Jadhav* case, the oral hearing took place 7 days after the request was filed, and the order was delivered 3 days after the oral phase. In *Armenia v Azerbaijan (First Request)* case, the request was filed on 16 September 2021, the oral hearings were scheduled for 14 and 15 October 2021, and the order was delivered on 7 December.

But what if the case is highly urgent? This was precisely the situation in the *LaGrand* case, where it took approximately 24 hours from the request to the order. The Court made use of the procedure under Article 75(1) of the ICJ Rules and imposed measures *proprio motu* to bypass the oral phase. The judges communicated by phone, which was considered a sign of the times.

There are other proceedings where the necessity for urgent processing is hard to deny, such as *Tehran Hostages* and *Ukraine v Russia 2022*. As the Court is reluctant to use Article 75(1), are there any other solutions? Article 59(2) of the ICJ Rules, introduced during the COVID-19 pandemic, appears to be quite useful. It allows for the oral phase to be conducted entirely or partially by video link. Given the limited likelihood of obtaining measures under Article 75(1), this provision may very well represent the future of proceedings. Implementing video links would streamline the scheduling of the oral phase and, consequently, expedite the delivery of orders.

This presentation aims to examine and analyze how the utilization of new technologies, such as video links under Article 59(2) of the ICJ Rules, can influence the Court's capacity to preserve the sense of urgency in provisional measures proceedings.

9 ILEGOGIE OSHOKHA -

BRIDGING THE GAP: A LEGAL ANALYSIS OF THE IMPACT OF ARTIFICIAL INTELLIGENCE (AI) ON THE RIGHT TO HEALTHCARE AND UNIVERSAL HEALTH COVERAGE (UHC) IN DEVELOPING COUNTRIES

This research paper focuses on the legal facets of incorporating Artificial Intelligence (AI) into healthcare systems. It scrutinizes the possible advantages and legal complexities that arise when utilizing AI as a means to achieve Universal Health Coverage (UHC). The study explores how AI can enhance healthcare accessibility, efficiency, and quality, all while considering ethical and regulatory factors, particularly in developing nations. The primary objective of the paper is to establish a connection between AI advancements and the pursuit of UHC. By doing so, it provides valuable insights into the essential legal framework necessary for the responsible and fair integration of AI within healthcare systems.

10 GOMAA MOHAMED - *DIGITAL TRANSFORMATION AND ACCESS TO JUSTICE*

With the outbreak of the Covid-19 pandemic, many challenges aroused before the justice sector and citizens became frustrated with the current model of justice infrastructure. Therefore, most of institutions began looking for non-traditional solutions, (ex: Digital Transformation (DT), "Artificial Intelligence (AI), and others) to ensure the accessibility to its services, in a time-effective and uninterrupted way.

The research develops an international overview of E- justice, with a focus on DT effects on the efficiency and without prejudice to the rule of law. It runs cross-sectional data analysis for about (40) countries to measure the effect of technology on the access to justice, taking into account Number of Judges (NJ), Budget (Bud) and Disposition time (dt).

According to WJP's recent report 2019 measuring the Justice Gap, 1.4 billion people worldwide have unmet civil and commercial justice needs. Of the estimated 36% of people in the world who have experienced a non-trivial legal problem in the last two years, more than half (51%) are not able to meet their civil justice needs. Almost, vulnerable groups or with financial barriers (including low-income populations, recipients of government benefits, and the unemployed) are affected disproportionately and more likely to have difficult accessibility.

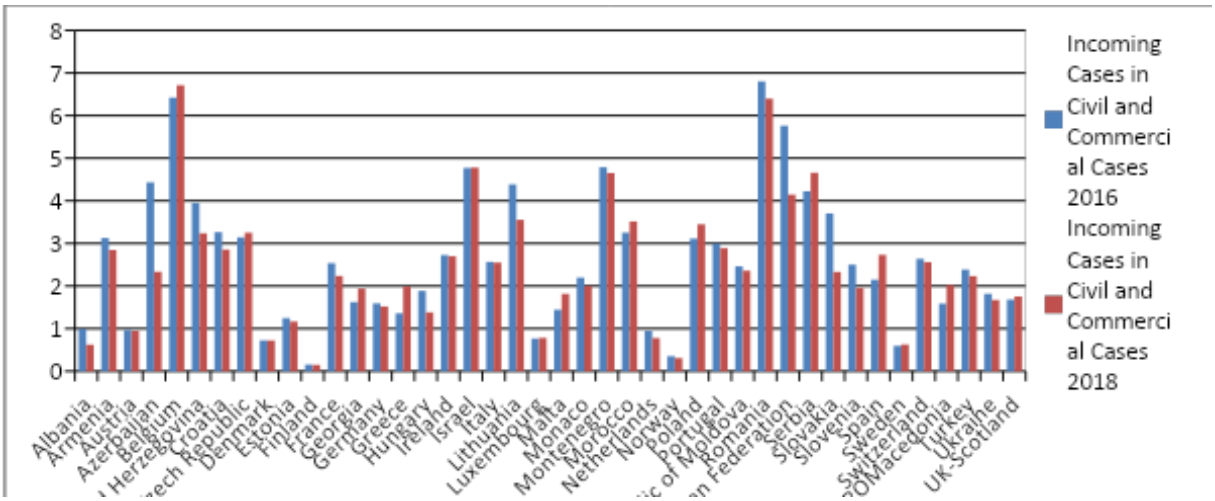

Figure 1: Source: **(Stata CEPEJ).**

This figure refers to the number of incoming first instance civil and commercial litigious cases per 100 inhabitants in 2016-2018, as a tool in our model to measure the access to justice. The median of incoming cases in European jurisdictions is 2.5 per 100 inhabitants (2016) and 2.3 in (2018), whereas the average value decreased slightly from 2.6 (2016) to 2.5 (2018) at received cases per 100 inhabitants.

Moreover, there are about (7) States and entities reached moderately low values, not exceeding one incoming case per 100 inhabitants. These are Albania, Finland, Luxembourg, the Netherlands, Austria, Denmark, Norway and Sweden.

Overall, the research confirmed the results of having a significant positive relationship between using Technology and access to justice with some observation. When judicial efficiency is measurable, it can be compared across individual judges, courts, districts and even across entire countries.

11 GUDAJCZYK MARCIN - *DIRECT CROSS-BORDER REQUESTS FOR DISCLOSURE OF ELECTRONIC EVIDENCE BY ICT SERVICE PROVIDERS - AN INSTRUMENT OF ENHANCED COOPERATION OR A THREAT TO HUMAN RIGHTS AND THE RULE OF LAW?*

The modern world increasingly relies on the use of digital technologies, especially the Internet and ICT services. A natural consequence of this is the observed rapid growth of the phenomenon of cybercrime, which is currently one of the most serious threats to individual goods protected by law, as well as to the legal system in general.

This situation is particularly noticeable in the practice of the judiciary and public prosecution. The specificity of cybercrime means that more and more evidence of crimes exists or is stored only in electronic form in IT systems. However, these systems often fall under the jurisdiction of a state other than the one in which the criminal proceedings are being conducted.

This, together with the need to preserve the evidence immediately, often makes obtaining it through traditional mutual legal assistance much more difficult or even impossible. Therefore, new measures need to be introduced to enable judicial authorities to quickly obtain evidence through cross-border cooperation mechanisms, including direct requests to foreign digital service providers.

The aim of the paper is to present the current state of the international community's attempts to meet the above-mentioned needs and to address the indicated issues through legal means in a way that, on the one hand, enables effective cross-border cooperation, especially between the public and private sectors, and, on the other hand, ensures the minimization of the risk of violations of human rights and fundamental freedoms that could be associated with the use of these mechanisms.

The reflection will be based on two normative legal acts - the Second Additional Protocol to the Cybercrime Convention on enhanced co-operation and disclosure of electronic evidence and the draft Regulation of the European Parliament and of the Council on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings. During the presentation, the mechanisms and tools for securing digital evidence containing subscriber and user data, traffic data, and content data, as well as their collection and transmission by private entities at the request of foreign law enforcement authorities, will be discussed, along with the proposed measures for supervision of the application of the aforementioned procedures.

Controversies and threats related to the adoption of the rules in question will also be presented, both from the perspective of international fair trial standards and the obligations imposed on states and their authorities in the area of privacy and personal data protection. The culmination of the presentation will be an (open-ended) attempt to answer the question of whether the proposed regulations will indeed enable the underlying objectives of their introduction to be achieved, and whether the accompanying safeguards for the protection of human rights and the rule of law will provide sufficient protection against excessive interference by judicial and law enforcement authorities.

12 KOULOUFAKOS TRIANTAFYLLOS - *INTERNATIONAL LAW ATTEMPTS TO PROTECT CRITICAL INFRASTRUCTURES AGAINST MALICIOUS CYBER OPERATIONS*

The vulnerability of critical infrastructures against cyber threats has been a problem yet to be seriously addressed, let alone be solved. Nevertheless, international law seems to play an awkward role in protecting critical infrastructures. Malicious cyber operations, especially against critical infrastructures, remain a gray area, with extremely harmful consequences. This paper will explore alternative international law avenues which could be used to protect critical infrastructures from malicious cyber operations during peacetime. Namely, it will examine the due diligence obligation and the non-intervention principle.

One of the ways international laws may assist towards an effective protection of critical infrastructures is through the application of the obligation of due diligence which is a general principle of law. Due diligence works through introducing positive obligations upon states to prevent unlawful situations. Thus, it could be argued that states have an obligation to take measures to protect their critical infrastructures. Nevertheless, the 2014 and 2016 International Law Association Study Groups on Due diligence found that due diligence is understood and applied differently, according to the sector in question. Even though states have agreed that the obligation of due diligence applies to cyberspace, they disagree on the way it is applied. The (non)-response to numerous cyber operations attributed to different states have shown that states are only willing to make some carefully worded statements regarding the application of the due diligence principle but are much less likely to comply with this obligation in a concrete situation. There are examples of states that have proclaimed that according to their view, the due diligence obligation applies in cyberspace, yet they constitute a minority which does not include major cyberspace powers like the US and China.

Another international law rule that could be pertinent to the protection of critical infrastructures, is the principle of non-intervention to the internal affairs of another state. It has been argued, and it is also affirmed by states, that the formulation of the non-intervention principle is wide enough to allow its application in cyberspace. In addition, it has been argued that malicious cyber operations may constitute coercion, which is the main requirement for a prohibited intervention. In that regard, it has been put forth that for a cyber operation to be considered coercive, a lower threshold of severity must be reached compared to cases of non-cyber intervention. In addition, the attacks must go against the "*domaine reservé*" of the country. This avenue seems to be gaining some traction, as a small number of countries in their published views on the way international law applies to cyberspace, suggest that a cyber-attack on their critical infrastructures would violate the principle of non-intervention. The aforementioned position may have little support, even so, it constitutes a small example of state practice which, if followed by more states, may lead to a formation of customary international law.

13 LASA ROBERT - *INDIVIDUAL RESPONSIBILITY FOR WAR CRIMES COMMITTED IN CYBERSPACE UNDER DOMESTIC CRIMINAL LAW AND INTERNATIONAL CRIMINAL LAW*

The purpose of the paper is to identify limitations affecting the criminal prosecution of an individual who commits war crimes in cyberspace. The rationale for it is the fact that there are no attempts to prosecute individuals because of war crimes committed in the cyberspace or the absence of appropriate legal rules rendering it possible to prosecute them. The analysis will be based upon the regulations of domestic criminal law in selected states, i.e. the United States, the Russian Federation, the People's Republic of China, Great Britain, and also upon the regulations of international criminal law. The criterion according to which these states were selected is their military potential in terms of conducting military activities in the cyberspace, which has already been confirmed, for example, by the American cyberattack on an Iranian nuclear facility in 2010. Moreover, as the criterion according to which these states were selected was the attitude of the above-mentioned states towards the Rome Statute of the International Criminal Court. The first three states are not parties to the Statute, whereas the UK ratified it in 2001.

The analysis is based on the main research question 'How to bring to justice a hacker for war crimes committed in the cyberspace effectively?'. A research question formulated this way renders it possible to formulate a hypothesis according to which individuals perpetrating war crimes connected with military operations in the cyberspace are not facing criminal responsibility because of the lack of effective and uniform legal solutions rendering it possible to conduct criminal proceedings against them, both in accordance with domestic and international alike. Analysing the hitherto activity of hackers in the course of armed conflicts, it should be indicated that they need to be divided into two groups. The first of them includes special-purpose army units, being parts of the secret services. At multiple occasions, the responsibility of this unit for cyberattacks against Ukrainian power grid, which deprived civilians of power supply. The second group is composed of private persons, the majority of whom are not formally connected with the armed forces. Such a situation occurred in Georgia in 2008, when Russian military were supported by the group Russian Business Network, conducting secret operations in the cyberspace, with public institutions, like the Georgian Ministry of Foreign Affairs. Those persons, just like the members of the armed forces, are responsible for the war crimes committed by themselves. A challenge faced by contemporary criminal law is how to institute a criminal procedure against a hacker if the hacker in question was following orders issued by a state in the course of an armed conflict and the state is reluctant or unable to bring them to justice.

The basic method of conducting the research is the dogmatic method, which made it possible to analyze the norms of international law, established at the global and regional level, as well as national law. The complementary role is played by the theoretical method, which indicates the position of doctrine and the content of legally non-binding documents.

14 KRAUSOVÁ PAVLÍNA - *TAX AND TECHNOLOGY IN DEVELOPING COUNTRIES*

This article aims to provide an understanding of technology's significance in mobilising tax in developing countries. While resources are often scarce in these countries, the use of technology can significantly improve the efficiency of tax authorities.

One of the challenges that developing countries face is the lack of access to relevant data and its timely and efficient processing. This makes it challenging for tax authorities to conduct complex proceedings against large multinational corporations. Additionally, cross-border cooperation between tax authorities is often required to reduce cases of tax evasion and harmful tax optimisation, which is a common issue faced by developing countries due to the complexity of the global economy.

Although tax policy has traditionally been the domain of sovereign states, international cooperation has a direct impact on national tax systems. International treaties often contain specific goals and standards that national tax authorities must follow. While each country has its unique set of challenges, some issues can be generalized, such as the scope of taxpayer data protection, taxpayers' right to privacy, and the role of big data.

Concerns of potential abuse or corruption limit the scope of powers available to public authorities or a full and automated cross-border exchange of information. This is particularly true for developing countries, which face distinct obstacles in this regard. It is crucial to address these concerns to ensure fair and effective tax systems.

At the international level, the UN Tax Committee plays an important role in working with developing countries. Additionally, UNDP and OECD have launched the project of Tax Inspectors Without Borders, which provides practical approaches and training to tax authorities in developing countries to help them overcome the challenges they face in mobilizing tax. These initiatives can help promote the interests of developing countries and ensure their fair share of tax revenues.

While the critical role of technology has the potential to promote the interests of developing countries, there are still relevant legal issues to be addressed. For instance, what data are we willing to share effectively to reduce the current systemic gaps, and among which countries? How can we ensure the reliability, timeliness, and protection of this data? How can we ensure adequate training of government officials and their access to technology? Finally, what are the values of our future tax cooperation that would further empower the developing countries? These are essential questions that need to be addressed to ensure the effectiveness of technology in tax mobilisation in developing countries.

In conclusion, technology has a critical role in tax mobilisation in developing countries. It can improve the efficiency of tax authorities, which is of utmost importance in countries where resources are scarce. However, there are still relevant legal issues that need to be addressed to ensure fair and effective tax systems. International cooperation, such as that provided by the UN Tax Committee and the Tax Inspectors Without Borders project, can help promote the interests of developing countries and ensure their fair share of tax revenues.

15 PAPACHRISTODOULOU

APHRODITE - *BORDER DEATHS ON THE RISE? THE EXERCISE OF STATE POWER THROUGH REMOTE CONTROL MECHANISMS*

The 'migration crisis' has once again been thrust into the spotlight in what can be described as the second deadliest shipwreck on record in the Mediterranean since the April 18, 2015, migrant shipwreck off Libya that killed some 1,100 people. This time, the incident unfolded outside Greece, near the tourist destination and coastal town of Pylos, with approximately 600 people missing/presumed dead. The calls to end the practice of non-assistance at sea, which undermines well-established obligations of international law of the sea are countless. The Pylos shipwreck is an appalling illustration of the ongoing failure of the EU and its Member States both to address the structural causes of the increasing number of border deaths and to provide a humanitarian migration response in the context of external border management.

The paper begins to undertake a human rights analysis of the increasing number of lives lost in the Mediterranean while trying to irregularly cross the borders of Europe. In doing so, it examines contemporary practices of State power that have been increasingly witnessed through the use and deployment of technologies in external border management. The notable operational shift of migration management to the digital realm reflects the strategic priorities of the Union and its Member States to drastically strengthen the control of external borders by creating a technological infrastructure of surveillance that ultimately serves as an accountability avoidance tool. This, in turn, has unveiled a new generation of human rights violations, where States activities beyond their territory (including their territorial waters) fall in a black tech-hole and have created a vacuum in human rights protection at sea. The paper seeks to provide an understanding of how sophisticated technologies used at maritime borders have a negative impact on the human rights of migrants – and lives. At the same, it aims to change the narrative to 'smartening human rights protection' by arguing that technologies can be perceived as remote control mechanisms that induce effects of power over migrants at sea, triggering in this way extraterritorial human rights obligations.

16 PANIGAJ JURAJ -

INTERNATIONAL LEGAL MECHANISMS OF THE PROTECTION OF BIOLOGICAL DIVERSITY IN THE CONTEXT OF CURRENT TECHNOLOGIES

The increasing complexity and urgency of global environmental challenges have prompted the international community to seek innovative solutions. Technology, with its rapid advancements and transformative potential in recent years, has emerged as a critical tool in addressing these pressing environmental issues, but on the other hand, in certain scenarios it poses a threat to the environment. At the beginning, contribution explores the role of technology in the context of international environmental law in general. The main objective is to analyze the relationship between technology and the legal protection of biological diversity of animal and plant species. To achieve the set objective, article firstly examines the recent technological development that could possibly have an impact on the protection of the biological biodiversity. Subsequently, the article analyzes the most important international environmental treaties, but also the most current international agreements, such as the Convention on the Law of the Sea on the conservation and sustainable use of marine biological diversity of areas beyond national jurisdiction. In relation to the international treaties, contribution examines the ability of existing treaty law to respond to technological development bearing in mind that legal frameworks often struggle to keep pace with the rapid evolution of technology, necessitating flexible and adaptive approaches. In the final part, the article summarizes the potential influence of technology on international environmental law, specifically protection of the biological diversity, highlighting its contributions, challenges, and prospects. Furthermore, article does not neglect even the analysis of potential risks associated with certain technologies that may exacerbate environmental problems.

17 POLLARD MIKE -

REGULATING ARMED SWARMS UNDER INTERNATIONAL LAW

Robotic swarms generally behave in a way that is synonymous with those found in nature. But, while the contemporary mechanical incarnations have bee7n touted as a method for tackling issues such as the decline in natural pollinators, the technology is also being militarized. The resulting armed swarms remain (for the most part) at the developmental stage. However, these are particularly controversial and their lawfulness under International Humanitarian Law (IHL) contended.

A key obstacle in determining the lawfulness of such weapons is their adaptability. Generally, each member is identical, providing the advantage that swarms have no 'leader'. This means the larger body can continue to function where individual members become inoperative. Moreover, individual members can change their behaviour based upon information collected by the group. This means that armed swarms can be deployed in a variety of ways. They might, for example, act as cloak - each member being a sacrificial decoy tasked with protecting a high value payload. However, a swarm might also be deployed into an environment - each member being capable of applying a lethal force to an individual or object that is selected according to certain predefined criteria.

From an IHL perspective, armed swarm deployments can arguably be justified. The simplest retort being that if swarms were programmed to strike only legitimate military targets (e.g., tanks) the principle of distinction is adhered to. To some extent, this argument is supported. Armed swarms may, however, be given a similar, but alternative instruction, such as kill all males of military age.

With the latter in mind, the presentation will demonstrate that such deployments may have the effect of spreading terror among the civilian population (noting if terror was the primary objective, the deployment would be prohibited by IHL). Attention will also be drawn to the notion that certain deployments may violate human rights obligations such as the right to liberty and security of person.

However, a rule that has, thus far, been overlooked is Art. 51(5)(b) AP I. The presentation will demonstrate that this provision may be key to regulating armed swarms because an attack of this type could be defined as a "bombardment". In this regard, the presentation will refer to the drafting history to identify concerns that might be relevant today. In addition, however, the literal definition will be examined, one such definition providing a bombardment is "a continuous attack with either bombs, shells, or other missiles" (missiles being defined as objects "forcibly propelled at a target either by hand or from a mechanical weapon").

The primary objective of the presentation is to demonstrate that if armed swarm deployments can be defined as bombardment, or alternatively, where they can be identified as a method or means of warfare which treat as a single military objective a number of clearly separated and distinct military objectives, they must be considered indiscriminate and therefore unlawful weapons. And while this may not altogether prevent armed swarm deployments in conflict, it may greatly restrict them.

18 RAJTR JIŘÍ – *GEOFENCING: NEW CHALLENGE IN INTERNATIONAL RESPONSIBILITY*

No past military conflict was so strongly shaped by off-the-shelf technologies as the war in Ukraine. Mobile phones, social networks, and mainly drones have become symbols of this conflict. Many technologies used and operated on the front lines are imported from other countries, and those countries still have a say in the way they are used—by geofencing.

These days, almost all commercial drones have software installed by the manufacturer that prohibits the drone from entering certain areas. It is done mainly to protect critical installations, such as airports and nuclear power plants, and the respective airspace around them from drones interfering with these kinds of installations. However, manufacturers, such as DJI, can update those geofencing rules to include more installations or to ban such drones from flying in an entire country (as has been seen in 2017 when such a ban was put in place over Iraq and Syria). But, to this day, no such restriction has been put in place over Ukraine. Even though DJI executives made statements in which they resented the use of their products in military operations, both sides of this conflict are putting those drones to use not just for reconnaissance but also to drop small explosive munitions into the trenches of the enemy.

On the other hand, Starlink, a satellite internet network owned by SpaceX, did use geofencing to limit its services. This was done at the same time, as the Ukrainian military relies on Starlink for communications and for drone operations on the front lines. This can have a strong impact on military operations that are happening in those regions.

Both cases illustrate the power that manufactures, and service providers respectively have by geofencing their products. As both examples mentioned are from countries that are not party to this conflict, an important question arises – Can those corporations or states, in which these corporations are based, be responsible for actions that were allowed by (not) geofencing?

19 SABJÁN NIKOLAS - *EU CYBER SANCTIONS: CURRENT INTERNATIONAL LEGAL CONTROVERSIES AND FUTURE PROSPECTS*

Sabján Nikolas

Cyber sanctions are a relatively new phenomenon closely connected to the rise of new digital technologies. In particular, cyber sanctions have been adopted by major powers (e. g. US, EU) as a reaction against malicious cyber activities. Both the EU and US have already adopted legal framework concerning cyber sanctions. However, several international legal issues pertain to the imposition of cyber sanctions which have been address by the existing academic literature. The aim of this article is to contribute to this scholarship.

First, I will introduce the janus-faced character of new digital technologies in the context of sanctions. Namely, I shall point out that the new technological developments may undermine the effectivity of sanctions, as these may be evaded through cryptocurrencies, Blockchain or other technologies. At the same time, different technological developments may prove to be useful when it comes to the enforcement of sanctions (e. g. by using AI for sanctions screening). Thus, while the existing literature tends to emphasize the negative impact of new technologies on the effectivity of sanctions, I argue that the picture is more nuanced and the said pessimism is not entirely warranted.

Secondly, the article will provide a working definition of cyber sanctions and analyse the recent state practice in this sphere, focusing more closely on the EU's practice and discuss some of the difficulties with the EU's legal framework on cyber sanctions from international legal perspective.

Subsequently, I will turn to and discuss my main argument/hypothesis, i. e. that the imposition of cyber sanctions will gradually increase as a response to malicious cyber activities (here I also include the category of sanctions in the digital sphere). I argue that there are two reasons for this: first, there is a high probability that malicious cyber activities will increase, considering the current geopolitical competition between the US, EU, China and the emerging new powers, and furthermore, an ever-increasing number of activities are being shifted to the digital sphere which creates new „possibilities" for more malicious cyber activity and simultaneously, new forms of cyber sanctions; and secondly, the existing state practice seems to support the proposition that states (victims of cyber-attacks) are reluctant to officially attribute these acts to specific states. This is due to the uncertainties of attribution under the current international legal framework (ARSIWA). Nevertheless, another reason for this is that cyber sanctions provide a relatively comfortable tool for states to react against and deter future malicious cyber activities. It provides a certain leeway for states as there is a lack of state practice in this area and a relative paucity of legal regulation. Nonetheless, several legal problems are still present, for instance those pertaining to international legal justification of these measures or fundamental rights, which I shall discuss in the last part of the article.

20 STARKOWSKA AGATA -

MANIFESTATIONS AND CONSEQUENCES OF THE VIOLATIONS OF THE INTERNATIONAL LAW STANDARDS ON CYBER SECURITY IN THE CONTEXT OF THE WAR IN UKRAINE

The issue of international regulation dedicated to cybersecurity was prompted by one of today's most notorious conflicts, namely the war in Ukraine fought since February 2022. This conflict significantly affects both the political and legal space and, in addition, carries great social significance, making the topic of the war in Ukraine and manifestations of violations of international norms globally universal and close to everyone.

The aim of the considerations undertaken is to discover and analyse the consequences that violations of international norms in the field of cyber security cause. Subject-wise, the author will therefore focus on the regulations of international law dedicated to cyber issues and the sanctions provided for violations of these norms.

The starting point will be international standards aimed at ensuring cyber security, primarily arising from agreements between states at the United Nations. The addressees of these standards include Russia and Ukraine. The analysis will focus on the provisions of the UN Charter and the final reports of the UN Open-ended Working Group and the UN Group of Governmental Experts (Framework of Responsible State Behaviour). A benchmark will also be the so-called Voluntary Confidence-building Measures set up within the framework of the Organisation for Security and Co-operation in Europe.

A general analysis and assessment of the norms established under the above-mentioned acts will then be set in the context of the movements that have taken place during the Russian-Ukrainian conflict. It will be impossible not to mention on this occasion the ongoing war in the perspective of its political background and chronologically present the key hostilities to date.

The author will then look at the sanctions that have so far been slapped on Russia in the face of the country's breach of its international cyber-security obligations. Both economic and, above all, technological sanctions will be taken into consideration. Here, the concept and nature of a technological sanction' will be further clarified. The main point of reference will be the sanctions initiated by the European Union and those imposed by the US. In addition to analysing sanctions as a direct result of violations of international norms dedicated to cyber-security matters, the author will try to foresee further potential effects of the listed hostilities in both political and economic contexts. The essence of the consideration, however, will be primarily an examination of the long-term effects of the conducted cyber attacks and violations of international law norms on the establishment and application of such regulations, including the anticipated strengthening of cyber security protection.

The final considerations will lead to conclusions regarding the role cyber attacks play in war today.

Conclusions will also relate to how effectively international law counteracts and fights cybercrime.

Due to the author's affiliation, the position of Poland and other countries located close to the territory where the Russian-Ukrainian conflict is taking place will be signalled at the end. First and foremost, the role played by an event dedicated to the above-mentioned issue, namely the Cybersec Forum, which took place in Katowice this year, will be mentioned.

21 SKALSKI SZYMON - *CROSSING CYBER BORDERS: NAVIGATING A PATH TO INTERNATIONAL CYBER DEFENSE*

This paper examines the ongoing development of the UN Global Cybercrime Treaty, with a particular focus on how it compares to the 2001 Budapest Convention. The primary objective of this paper is to critically assess the draft treaty and its potential impact on international cybersecurity, particularly in addressing the pressing issue of transnational cyber-attacks.The primary objective of the paper is to critically assess the draft treaty and its potential impact on international cybersecurity, with a specific focus on addressing the pressing issue of transnational cyber-attacks.

Transnational cyber-attacks encompass a range of malicious activities, such as hacking attempts, data breaches, distributed denial of service (DDoS) attacks and ransomware incidents, orchestrated by actors operating from one country but targeting assets or systems in another. Due to their transnational nature, these attacks pose significant challenges in terms of attribution, enforcement of legal consequences, and protection of states and their critical infrastructure. They also pose a significant risk of massive financial loss.

This paper will focus on key issues related to cross-border cyber-attacks in the context of public international law. One such concern is the problem of jurisdiction and the attribution of specific attacks to particular countries. The anonymity and geographical obfuscation tactics used by cybercriminals, such as proxy servers and anonymisation tools, make it very difficult for victim states to identify the origin of attacks and hold perpetrators accountable. The study will also examine preventive measures and defence mechanisms that states can employ. Forensic and offensive measures to recover lost data will be examined for their potential importance in countering cyber threats. The study will analyse the effectiveness of the mechanisms proposed in both the draft UN Cybercrime Convention and the Budapest Convention.

A crucial aspect to be considered is the establishment of an effective network for information exchange and cooperation. While the EU is currently developing a network of Computer Security Incident Response Teams (CSIRTs) and a system for exchanging information on cyber security threats, it is important to explore potential mechanisms at the international level that can facilitate a more effective exchange of information in order to comprehensively address global cyber attacks.

In conclusion, this paper aims to assess existing and forthcoming proposals to regulate international consensus on joint responses to cybercrime threats. The focus will be on evaluating the effectiveness of existing and planned solutions and proposing alternative approaches, with particular attention to European solutions as potential models. Consequently, the research will compare international trends with the European approach, identifying similarities and differences in order to provide comprehensive insights into the global cyber security landscape.