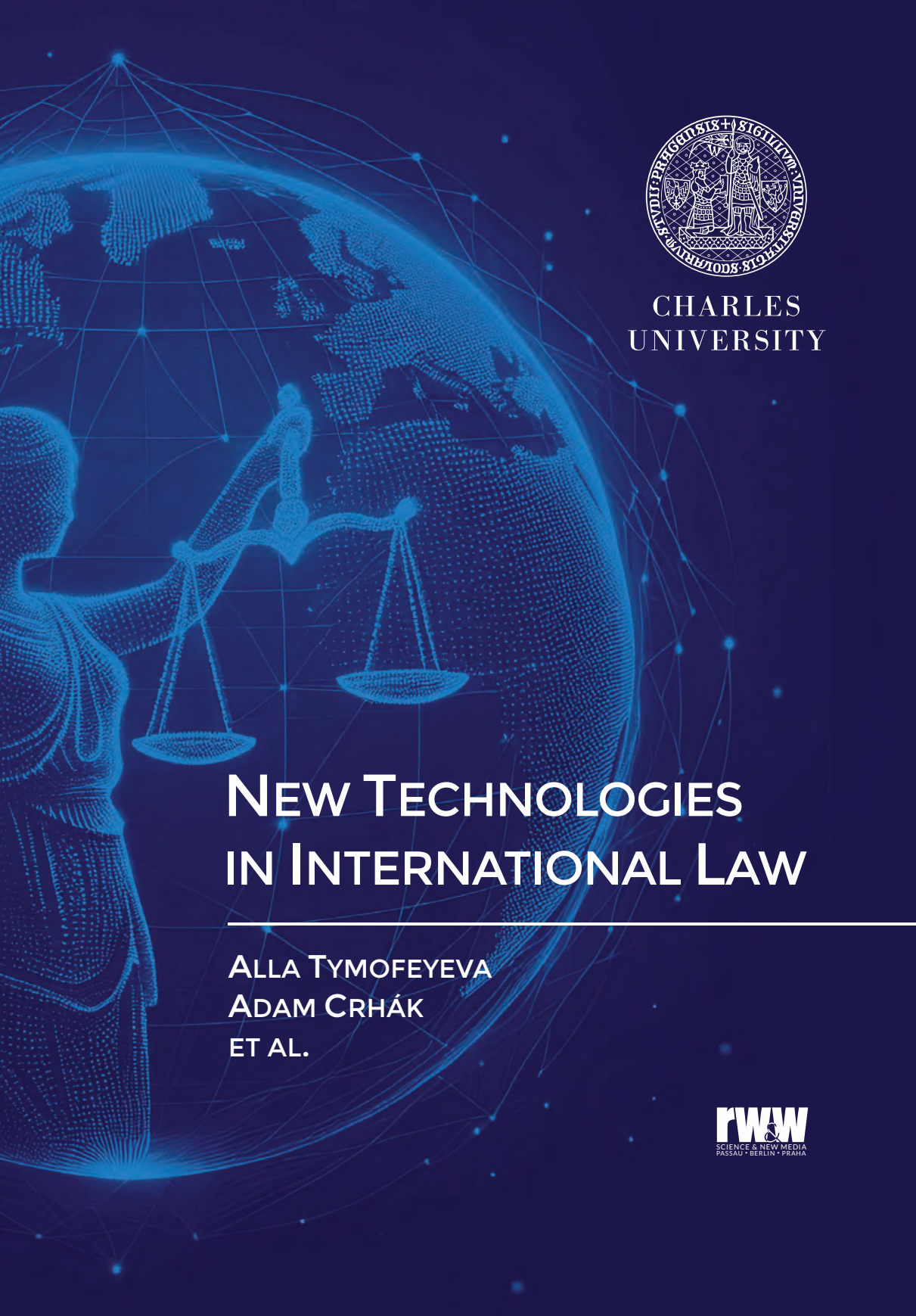


CHARLES
UNIVERSITY

New Technologies in International Law

Alla Tymofeyeva
Adam Crhák
et al.

rww
SCIENCE & NEW MEDIA
PASSAU • BERLIN • PRAHA

ELECTRONIC PUBLICATION CREATED BY
rww BOOK
SCIENCE & NEW MEDIA
PASSAU · BERLIN · PRAGUE

Interactive e-book
available online on cloud:
https://cld.bz/F36giRe

NEW TECHNOLOGIES IN INTERNATIONAL LAW

ALLA TYMOFEYEVA
ADAM CRHÁK
et al.

2024

Editors:

JUDr. Mgr. Alla Tymofeyeva Ph.D.

Adam Crhák

an international publishing project of SüdOst Service GmbH,
Am Steinfeld 4, 94065 Waldkirchen, Bayern/Germany
and Eva Rozkotová Publishers, 266 01 Beroun, Czech Republic

ISBN 978-80-87488-55-3

TABLE OF CONTENTS

About the authors

Bakošová, Lucia is currently a researcher at the Institute of International Law and European Law, Faculty of Law of Pavol Jozef Šafárik University in Košice, Slovakia. She received her doctoral degree in 2020 with the thesis "International aspects of natural and industrial disasters" at the Faculty of Law of Pavol Jozef Šafárik University in Košice. Since 2021, she is a member of a research team working on the project "Green Ambitions for Sustainable Development (European Green Deal from the perspective of international and domestic law), with main focus on legal regulation of artificial intelligence and sanction mechanisms related to sustainable development and international law. Furthermore, she teaches courses related to Public International Law.

Bird, Charles Ross is lecturer at Charles University, Faculty of Law in Prague, Czech Republic. He teaches Equity and Trusts, Criminal Law, and Legal English. He is currently a Ph.D. student at Charles University with an emphasis on property rights of celestial bodies. He earned his Doctor of Jurisprudence from Washburn University School of Law in Topeka, Kansas in the United States and earned his Master of Laws the University of Kent in Canterbury, England.

Byczyński, Michał is an Attorney-at-law Trainee and is a Ph.D. candidate at University od Lodz, Poland. In his studies he specializes in the field of public international law and his main interests include comparative legal studies, international standards of human rights protection and philosophical basis of international law. He is an alumnus of The Hague Academy of International Law.

Crhák, Adam is a law student in his final year of master's and has been a research assistant at the Department of International Law at the Faculty of Law of the Charles University in Prague for most of his studies. His main interests in international law lie in the use of force and different aspects of humanitarian law, especially the law of targeting and use of human shields in armed conflicts. He is currently furthering his academic pursuits on a study program in The Hague.

D'Evereux, Veronika holds JD and Ph.D. in Public International Law at Charles University in Prague, Faculty of Law. Her research is focused on multiple legal issues related to the Israeli Palestinian conflict from the perspective of international law. She works as a research fellow at the Charles University Centre for Conflict and Post-Conflict Studies. She also works as an immigration lawyer at the Integration Centre Prague and cooperates with private university CEVRO Institute in Prague.

Gerle, Marek is a Ph.D. candidate at the Faculty of Law of the Charles University in Prague. In his research, he focuses on the use of force in international law, precisely in connection to the phenomenon of de facto states. Besides this, his interests include the international criminal law and specifically the crime of genocide. Recently, he enriched his research during academic stays at the Ivane Javakhishvili Tbilisi State University, Georgia and Université de Côte d'Azur, France.

Gomaa, Mohamed is a Judge at the Court of Appeal, Egyptian Ministry of Justice, an expert at the European Legal Tech Association (ELTA), and aboard member of the

"CIArb (YMG) Global Steering Committee", a member of the scientific committee of International Journal of Legal Interpretative Judgement, published by the "Democratic Arab Center" Germany – Berlin and a former lawyer, the legal affairs department at the Egyptian Russian University.

Gudajczyk, Marcin is a graduate of Law and Arabic Studies at the University of Warsaw. He also completed academic internships at Cairo University and Kuwait University. He is a doctoral student at the Faculty of Law and Administration of the University of Silesia in Katowice, where he teaches European law and criminal law and is preparing his dissertation on countering the financing of terrorism in the legal systems of the Arab states of the Persian Gulf. Author of publications on legal issues of Arab countries, criminal law and forensics. Graduate of the Polish National School of Judiciary and Public Prosecution. He works as a sub-prosecutor at the District Prosecutor's Office in Katowice.

Ilegogie, Oshokha Caleb is a second-year PhD Student at the Faculty of Law, Charles University. His main area of expertise is healthcare law, but he also takes interest in legal policy and compliance. He received his bachelor's and master's degrees from Northumbria University in Newcastle.

Kouloufakos, Triantafyllos is a Doctoral Researcher at the Centre for IP & IT Law of KU Leuven. He holds an LLM in Public International Law from the National and Kapodistrian University of Athens (Greece) (summa cum laude) and an LLM in Public International Law from the University of Groningen (the Netherlands) (cum laude) for which he was also awarded the University of Groningen Talent Grant: Partial Scholarship Law 2020–2021. He has worked as a lawyer in Greece for 3 years. He was a part of the inaugural cohort of the European Cybersecurity Fellowship (2022–2023) of the European Cyber Conflict Research Initiative. He is mainly interested in issues of cyberspace accountability, the protection of critical infrastructures from malicious cyber operations and the use of norms and standards to regulate cyberspace. His PhD Project concerns the potential application of the no-harm principle in cyberspace in order to achieve a more effective harm redress from malicious cyber operations.

Krausová, Pavlína is a PhD candidate at Charles University, Faculty of Law. Her field of expertise consist mainly of international economical law and tax law. She has academic experiences from both University of Paris 1: Panthéon-Sorbonne and University Jean Moulin in Lyon.

Łasa, Robert is currently a Ph.D. student at the Doctoral School of the University of Silesia in Katowice in the field of international law. His dissertation covers the protection of critical infrastructure during the armed conflict. He actively participates in national and international scientific conferences and publishes research papers. In addition, he gains teaching experience by giving classes in international law and European Union law, as well as preparing students for moot court competitions (the All-European International Humanitarian and Refugee Law Moot Court Competition and the Helga Pedersen Moot Court Competition).

Panigaj, Juraj is currently a doctoral student at the Pavol Jozef Šafárik University, Faculty of Law, Institute of International law and European law, as well as a practicing

lawyer. As part of his doctoral studies, his research deals primarily with international legal mechanisms of the protection of nature, landscape and biological diversity of animal and plant species.

Papachristodoulou, Aphrodite is a Post-Doctoral Research Fellow at the Irish Centre for Human Rights, School of Law, University of Galway. She holds a PhD in law from University College Dublin, a Master of Laws in Maritime Law from University College London and an LLB from University of Southampton. Dr Papachristodoulou is a licensed lawyer (Cyprus Bar, 2016) and engages in strategic human rights litigation with non-governmental organisations. She further provides advice and interacts with the media on law of the sea and human rights issues in the migration domain. Her principal research interests include international human rights, law of the sea, migration and border technologies. She is also a Research Affiliate at the Refugee Law Initiative and a Committee Member of the International Law Association on the Protection of People at Sea (Irish Branch).

Pappa, Foto is a PhD candidate at the Sant'Anna School of Advanced Studies, researching digital agriculture and human rights. She holds an LLM in International Human Rights Law from the University of Groningen (cum laude) and an LLM in Public International Law from the National and Kapodistrian University of Athens (summa cum laude). She has been admitted to the Athens Bar Association.

Pollard, Michael J. is a lecturer in law, University of the West of England. His primary area of interest is related to new technologies, most especially Artificial Intelligence and autonomous robotic systems, will impact upon existing international law norms (use of force, international humanitarian law and international human rights law). Given the inherently interdisciplinary nature of this area of study, the researcher looks to engage with the fields of international relations, strategy, and ethics (amongst others) where possible.

Sabjan, Nicolas is an assistant professor at the Comenius University in Bratislava, Faculty of Law. He teaches legal theory and philosophy of law, and he has been responsible for supervising public international law moot courts. He holds a master's degree from Leiden University (LL.M, Public International Law) and he completed his PhD. in 2021 at the Comenius University, Faculty of Law. His research focuses on public international law, human rights law, and legal philosophy and theory.

Skalski, Szymon is a PhD candidate at Jagiellonian University in Krakow. His work to date includes publications in the fields of civil law, cyber security and artificial intelligence. He has also been collaborating for two years on a project on insurance contracts evolution in the 21st Century. His doctoral thesis is on the characteristics of a cyber attack from a tort liability perspective. He has also been working professionally for two years in cyber security regulatory consulting.

Starkowska, Agata is a student at University of Warsaw, Faculty of Law and Administration. She was a finalist of the Human rights Olympiad organised by University of Warsaw and published an article titled "The rule of law as an EU value - remarks on the normative and factual state of the rule of law".

List of abbreviations

Abbreviation	Definition
ADB	Asian Development Bank
AFIP	Argentina's tax administration
AI	artificial intelligence
AI Act	Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence
AILD	AI Liability Directive
AP I	Additional Protocol I to the 1949 Geneva Conventions
AP II	Additional Protocol II to the 1949 Geneva Conventions
API	Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts
ARSIWA	Responsibility of States for Internationally Wrongful Acts
ATAF	African Tax Administration Forum
AWS	autonomous weapons systems
BC	2001 Budapest Convention
BEPS	Base Erosion and Profit Shifting
CBD	Convention on Biological Diversity
CEPEJ	Council of Europe European Commission for the efficiency of justice
CESCR	Committee on Economic Social and Cultural Rights
CIAT	Inter-American Center of Tax Administrations
CoE	Council of Europe
CRS	Common Reporting Standard
DC	Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes
DoD	The United States Department of Defence
DT/ICT	Digital Transformation
ECtHR	Europeam Court of Human Rights
ELTA	European Legal Tech Association
EMP	electromagnetic pulse
EOI	Exchange of Information
EPOR	Council on European Production Orders and European Preservation Orders
ESRMs	Electronic Sales Register Machines
EU	European Union
EUROSUR	European Border Surveillance System
FAO	Food and Agriculture Organization

FCAI	Framework Convention on Artificial Intelligence, Human Rights, Democracy, and the Rule of Law
FIRS	Nigeria's tax administration
Frontex	EU's Border and Coast Guard Agency
GCC	General Claims Comission
GDF	Guardia di Finanza
GDPR	General Data Protection Regulation
GTP III	China's Golden Tax Project III
HIPAA	Health Insurance Portability and Accountability Act
IAC	armed conflict of an international character
ICC Statute	Rome Statute of the International Criminal Court
ICCPR	International Covenant on Civil and Political Rights
ICESCR	International Covenant on Economic, Social, and Cultural Rights
ICJ	International Court of Justice
ICRC	International Committee of the Red Cross
ICTs	Information and Communication Technologies
ICTY	International Criminal Tribunal for the former Yugoslavia
IDF	Israeli Defence Forces
IGE	International Group of Experts
IHAT	Iraq Historic Allegations Team
IHL	International Humanitarian Law
IHRL	international human rights law
IIOT	industrial internet of things
ILA	International Law Association
ILC	The International Law Commission
IMT Charter	Charter of the International Military Tribunal
INSD	Israeli National Security Doctrine
IOM	International Organization for Migration
IOTA	Intra-European Organisation of Tax Administrations
IOTA	Internet of things
ITLOS	International Tribunal on the Law of the Sea
ITU	International Telecomunication Union
LCGN	Libyan Coast Guard and Navy
LDCs	least developed countries
ML	machine learning
NDPA	Nigeria Data Protection Act
NDPC	Nigeria Data Protection Commission
NDPR	Nigerian Data Protection Regulations
NGOs	non-governmental organizations

NIAC	armed conflict of a non-international character
NITDA	National Information Technology Development Agency
OECD	Organisation for Economic Co-operation and Development
OST	Outer Space Treaty
OT	operational technology
PCA	Permanent Court of Arbitration
PCIJ	Permanent Court of International Justice
PLD	EU Product Liability Directive
Principles	Principles for the Ethical Use of AI in the UN System (2022)
R2HE	the right to clean, healthy and sustainable environment
RBN	Russian Business Network
RRI	Responsible Research and Innovation
SADC	Southern African Development Community
SAR	search and rescue
SAR Convention	International Convention on Maritime Search and Rescue
SDGs	Sustainable Development Goals
SII	Servicio de Impuestos Internos
SIMPES	Comprehensive System for Monitoring Payments Abroad for Services
SMEs	small and medium-sized firms
SSU	The Security Service of Ukraine
TADAT	Tax Administration Diagnostic Assessment Tool
The High Sea Treaty/HST	Convention on Biological Diversity and its protocol, the Cartagena Protocol on Biosafety, and the Agreement under the United Nations Convention on the Law of the Sea on the conservation and sustainable use of marine biological diversity of areas beyond national jurisdiction
TIWB	Tax Inspectors Without Borders
UAVs	unmanned aerial vehicles
UN	United Nations
UNCSI	United Nations Convention on Jurisdictional Immunities of States and Their Property
UNDP	United Nations Development Programme
UNGA	United Nations General Assembly
UNSC	United Nations Security Council
UNODA	United Nations Office for Dissamament Affairs
VCLT	Vienna Convention on the Law of Treaties
WHO	World Health Organization
WW II	World War II

New Technologies in International Law

By ***Dr. Inga Martinkute*** (Vilnius University)

The constant stream of technological innovations, ranging from consumer wearables and satellites to artificial intelligence systems, raises crucial questions about the relations between technology and international law that need to be analyzed from different perspectives.

If we look at the historical interaction between international law and the major innovations, such as printed books, airplanes, vaccines or nuclear weapons, we may conclude that technology in itself did not transform international law fundamentally, but it did shape and influence it, opening new branches of international law and new discourses. Thinking about more recent technological advances, we should ask ourselves if the internet changes international law, or do online hearings alter international law profoundly? The overarching answer will most likely be that "no, recent technological innovations, however fascinating, do not change international law in a fundamental way". However, these changes in international law arising from technological innovation have been subtle, gradual, and noticeable over the decades, and they are often intertwined with geopolitical changes.

Some areas of the international law domain are more prone to technology-induced changes. Those affected areas are often related to digitalization and faster communication. Those international law areas that rely on the collection, search, storage, analysis, management and interpretation of information and data are undergoing major transformations. International law is just coming to terms with data transfers, artificial intelligence and the regulation of social media. Also, international law is grappling with the fast pace of new military technologies and new methods for resource extraction and appropriation. Meanwhile, other areas of international law have become obsolete because those areas of life have become obsolete with the advancement of new technology. For example, with the decline of telegrams, there will be no need for the International Telegraph Convention of 1875.

In this new age, technology is not a neutral force, although it is often portrayed as such. Frequently, it is a potent tool that amplifies human capabilities, both for constructive and potentially destructive purposes. The same technology that facilitates autonomous vehicles and biometric access also underlies drone attacks, demonstrating the dual nature of these advancements. It is also easier to hide biases and mistakes behind technology. In this context, it is natural to ask, should there be limits to the power wielded by technology? Is it incumbent upon the international community to self-impose restrictions on the development and application of technology? Furthermore, how can these limitations be effectively extended to the international stage, where nations engage in a competitive race for power and technological dominance?[1] The digital divide even further complicates the relationship between technology and international law. Technology providers hold significant leverage, potentially

[1] Hillman JE, *The Digital Silk Road: China's Quest to Wire the World and Win the Future* (Harper Business, 2021), p 5.

exacerbating existing inequalities between nations, forming new dependencies and opening possibilities for new forms of influence and manipulation.

Addressing these issues requires not only deep technical knowledge but also forward thinking and a strong ethical base. While regulation is often perceived as limiting or prohibiting, it can also be empowering and enabling. Striking the right balance is crucial, as effective international regulation can foster innovation, protect human rights, and prevent the misuse of technology.

This collection of articles provides a fascinating glimpse into this new world of technology and international law. The volume offers several papers addressing international law related to the use of technologies in war and for security reasons. In chapter I, Triantafyllos Kouloufakos looks at legal frameworks for the protection of critical infrastructure, and Michael J. Pollard analyses the regulation of armed swarms. Meanwhile, in chapter VI, Agata Starkowska and Michał Byczyński analyze international laws‘ regulations on cyber security and defence. In chapter VI, Robert Łasa, Marek Gerle, Adam Crhák, and Szymon Skalski look at various international aspects of regulating cyber crimes, also related to the laws of war. Lucia Bakošová, Juraj Panigaj, Charles Ross Bird, in their respective contributions in chapter III, focus on how technology influences environmental law through the lenses of biological diversity, sustainable development and appropriation of outer space. Technological challenges arising for developing countries are addressed by Pavlína Krausová, Oshokha Caleb Ilegogie in chapter IV, while Nikolas Sabján contributes with the analysis of EU cyber sanctions. In chapter II, Mohamed Gomaa and Marcin Gudajczyk address the technological changes as well as implications for international judicial systems and access to justice. The final chapter is devoted to the interaction of human rights and new technology, where Foto Pappa, Veronika D’Evereux and Aphrodite Papachristodoulou analyze digital agriculture, artificial intelligence and border controls.

This new research on international law is vital for conceptualizing and realizing Europe‘s role in the current technological transformation. While almost all technology giants with capabilities and resources for groundbreaking innovations are located in the Americas and Asia, Europe, for good or for bad, is capable of regulating those innovations and exerting that influence far beyond its immediate territory.[2]

[2] Bradford A, *The Brussels Eff ect: How the European Union Rules the World* (OUP, 2019), p. 7.

Navigating the Pros and Cons of New Technologies in International Law

By ***Dr. Alla Tymofeyeva*** (Charles University)

As with any major development, new technologies come with both benefits and drawbacks that affect all aspects of society. In the realm of public international law, the impact of these advancements is especially profound as it leads to a transformation of the international legal order. This impact is visible within all the domains of public international law.

Starting with the area of ***international humanitarian law***, it can be said that on one hand, new technologies, such as drones and satellite imagery, have improved the monitoring[3] and enforcement of humanitarian law, allowing for better protection of civilians in conflict zones. Technology has also enabled the rapid dissemination of information to those in need during humanitarian crises. On the other hand, the deployment of sophisticated weaponry may result in breaches of international humanitarian law in areas of conflict. Furthermore, the effectiveness of international legal mechanisms in overseeing the utilisation of modern technologies in armed confrontations could be diminished as the Geneva Conventions and other humanitarian law conventions were not originally designed to anticipate the rapid advancement of military technologies.[4]

New technologies, such as forensic DNA analysis and digital evidence collection, have greatly enhanced the ability of international tribunals and courts to prosecute war criminals and perpetrators of mass atrocities. Technology has also facilitated the collaboration and sharing of information among international institutions facilitating the provision of ***international justice***. At the same time, the reliance on technology in the gathering of evidence in international criminal trials can raise issues of privacy and data security. Additionally, the use of new technologies in international justice may worsen disparities in access to justice for marginalised communities, those who do not have access to internet or the necessary e-skills.

Advances in space technology have opened up new opportunities for international cooperation and exploration in outer space. The development of international agreements and conventions, such as the Outer Space Treaty, has helped to establish a framework for the peaceful use and exploration of outer space. However, the increasing privatisation and commercialisation of space activities raise concerns about the equitable distribution of resources and benefits derived from outer space. Additionally, the lack of clear regulations and enforcement mechanisms for space activities has created challenges in ensuring compliance with ***international space law***.

---

3 Lyons J, 'Documenting Violations of International Humanitarian Law from Space: A Critical Review of Geospatial Analysis of Satellite Imagery during Armed Conflicts in Gaza (2009), Georgia (2008), and Sri Lanka (2009)' (2012) 94(886) *International Review of the Red Cross,* p. 739.

4 Zhou J, *Fundamentals of Military Law: A Chinese Perspective* (Springer, 2019), p. 494.

Technology has played a crucial role in monitoring and addressing environmental challenges, such as climate change and biodiversity loss. Innovative solutions, such as remote sensing and satellite imaging, have enabled better tracking of environmental indicators and the enforcement of ***environmental regulations***. Nonetheless, the rapid pace of technological development can also contribute to environmental degradation. The use of genetic engineering raises ethical and legal concerns about their potential impact on the environment and human health.

Technological development of security tools has enabled the detection and prevention of cyber-crimes,[5] such as hacking, fraud, and identity theft, etc. International cooperation and information sharing have also improved efforts to combat cyber threats across borders. However, the increasing interconnectedness of digital networks has created new vulnerabilities and risks for cyber-attacks, leading to challenges in enforcing international laws and regulations on cyber-crimes. The lack of appropriate legal framework further complicates efforts to address ***cyber threats at the international level***.

New technologies have a significant impact on the areas of ***international human rights law***. Technology has empowered individuals and civil society groups to document human rights abuses, amplify their voices, and hold governments and other actors accountable for violations. Social media platforms and digital communication tools have played a key role in facilitating advocacy and activism for human rights causes. However, the use of new technologies, such as surveillance systems and facial recognition technology, can infringe on individuals' right to private life.[6] The lack of regulatory safeguards and oversight mechanisms for the use of technology in the context of human rights can exacerbate risks of abuse and discrimination.

In conclusion, the proliferation of new technologies in international law brings both opportunities and challenges that necessitate a balanced approach towards harnessing their transformative potential while mitigating associated risks. With the growth of use of new technologies, it is imperative to prioritise ethical considerations, safeguard privacy and security, and foster inclusive and equitable access to legal resources, ensuring that the benefits of technological innovation are maximised while minimises adverse impacts on the rule of law and international justice. The recent adoption of the EU Artificial Intelligence Act[7] demonstrates the urgent need to regulate the use of new technologies for the sake of protecting fundamental rights, democracy and the rule of law.

---

5 Baggili I (ed), *Digital Forensics and Cyber Crime: Second International ICST Conference, ICDF2C 2010*, Abu Dhabi, United Arab Emirates, October 4–6, 2010, Revised Selected Papers (Springer Berlin Heidelberg 2011), p. 27.

6 Berle I, *Face Recognition Technology: Compulsory Visibility and Its Impact on Privacy and the Confidentiality of Personal Identifiable Images* (Springer, 2020), p. 39 and p. 89.

7 Artificial Intelligence Act, EU, P9_TA (2024)0138, 13 March 2024.

CHAPTER I

HUMANITARIAN LAW

1.1 Regulating Armed Swarms Under International Law

By ***Michael J. Pollard*** (University of the West of England)

Introduction

A variety of emerging weapons technologies such as hypersonic missiles,[8] loyal wingman systems,[9] electromagnetic pulse (EMP) weapons,[10] and laser weapons[11] have the potential to revolutionise military affairs.[12] Despite the military advantages these weapons offer however, they do not represent a significant challenge in terms of their compliance with international law when deployed in armed conflict. Instead, the military decision-maker responsible for authorising their deployment (present and/or future) will remain governed by the obligations contained within IHL, not least the principle of distinction.[13]

Of the known military systems currently under development,[14] however, perhaps the most controversial is Autunomous Weapons Systems (AWS).[15] Indeed, due, inter

[8] There is no strict definition of what constitutes a hypersonic missile, but it should be capable of travelling at speeds in excess of 3500mph. See e.g., Boyd I, 'How hypersonic missiles work and the unique threats they pose – an aerospace engineer explains' (*The Conversation*, 15 April 2022) <https://theconversation.com/how-hypersonic-missiles-work-and-the-unique-threats-they-pose-an-aerospace-engineer-explains-180836> accessed 7 November 2023.

[9] See e.g., Boeing, 'Loyal Wingman: Uncrewed but not alone' (*Boeing*, 23 November 2023) <https://www.boeing.com/features/innovation-quarterly/2021/11/boeings-loyal-wingman.page> accessed 1 November 2023.

[10] See, e.g., Mizokami K, 'The Army's New Drone Killer Can Fry Whole Swarms in Midair' (*Popular mechanics*, 7 November 2023) <https://www.popularmechanics.com/military/weapons/a45713388/us-army-new-drone-killer-leonidas/> accessed 14 December 2023.

[11] See e.g., Judson J, 'US Army awards Boeing, General Atomics contract to develop powerful laser weapon' (*Defence News*, 3 November 2021) <https://www.defensenews.com/land/2021/11/03/us-army-awards-boeing-general-atomics-contract-to-develop-powerful-laser-weapon/> accessed 21 October 2023.

[12] Revolution in military Affairs (RMA) is a term that is applied to a new technology that significantly changes the way war is fought. For example, the aircraft carrier, allowed nations to move their tactical and operational aircraft much closer to a battlefield, and more quickly than had previously been possible.

[13] Distinction, or the basic rule, is codified in Art. 48 Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977, 1125 UNTS 3 (hereinafter API). Art. 48 provides, 'In order to ensure respect for and protection of the civilian population and civilian objects, the Parties to the conflict shall at all times distinguish between the civilian population and combatants and between civilian objects and military objectives and accordingly shall direct their operations only against military objectives'. This principle is also considered to be customary in nature, see e.g., International Committee of the Red Cross (hereinafter ICRC), Customary International Law database, Rule 1, available at, <https://ihl-databases.icrc.org/en/customary-ihl/v1/rule1> accessed 31 October 2023.

[14] Noting that military technology is, for reasons that require little explanation, typically shrouded in secrecy.

[15] From what started as relatively niche discussion in 2007 (see generally e.g., Sparrow R, 'Killer Robots' (2007) 24(1) *Journal of Applied Philosophy* 62;
(Speaker T, O'Donnell S, Wittemyer G et al, 'A Global Community-Sourced Assessment of the State of Conservation Technology' (2022) 36(3) Conserv Biol 13871), there is now a wealth of discussion.

alia, to concerns about the inability of AWS to operate in adherence to IHL, various opponents are currently urging the UN to prohibit, or at the very least regulate, AWS by way of a new treaty.[16] Following a sustained period of pressure the UN General Assembly (UNGA) has even very recently adoptes its first ever resolution on AWS,[17] which identifies an "urgent need for the international community to address the challenges and concerns raised by autonomous weapons systems".[18]

The term AWS is, nevertheless, somewhat misleading because it is not used to identify a particular type of weapon. Instead, it is generally applied to any weapon that utilises AI to support its own decision-making processes. An AWS, simply put, is any weapon that can make its own decisions about who lives and who dies on a battlefield. There is no single widely recognised definition of AWS, which is a primary reason why it is also difficult to determine their overall lawfulness (or not). Nonetheless, a popular definition posited by the ICRC provides that an AWS is any weapon system that can,

> *select and apply force to targets without human intervention. After initial activation or launch by a person, an autonomous weapon system self-initiates or triggers a strike in response to information from the environment received through sensors and on the basis of a generalized "target profile".*[19]

Even for the non-expert, a brief analysis of the above text is likely to reveal it has the potential to encapsulate a wide variety of weapons (future and, arguably, existing).[20] These might include, for example, anything from smart grenade (which, for example, might be capable of choosing not to detonate based upon detecting the presence of civilians),[21] to hunter-killer drones (which might continuously circle the globe in search of 'high value' targets),[22] and even humanoid robots such as the infamous

---

A useful starting point is provided by NGO's such as, Campaign to Stop Killer Robots, 'Stop Killer Robots' <https://www.stopkillerrobots.org/>; Amnesty International, 'Global: A critical opportunity to ban killer robots – while we still can' (2 November 2021) <https://www.amnesty.org/en/latest/news/2021/11/global-a-critical-opportunity-to-ban-killer-robots-while-we-still-can/>; Article 36, 'Autonomous Weapons' <https://article36.org/what-we-think/autonomous-weapons/>; and Wareham M, 'Killer Robots' (*Human Rights Watch*) <https://www.hrw.org/topic/arms/killer-robots> each accessed 31 October 2023.

[16] See e.g., UN News, 'UN and Red Cross call for restrictions on autonomous weapon systems to protect humanity' (*UN News*, 5 October 2023) <https://news.un.org/en/story/2023/10/1141922> accessed 31 October 2023.

[17] UNGA, Res A/C.1/78/L.56 (2023) <https://documents-dds-ny.un.org/doc/UNDOC/LTD/N23/302/66/PDF/N2330266.pdf?OpenElement> accessed 7 November 2023. AWS are also referred to as Lethal Autonomous Weapons Systems (LAWS), Lethal Robotics, and Killer Robots amongst others.

[18] Ibid., UNGA Res. L. 56. See also United Nations Press, 'First Committee Approves New Resolution on Lethal Autonomous Weapons, as Speaker Warns "An Algorithm Must Not Be in Full Control of Decisions Involving Killing"' (*United Nations Press*, 1 November 2023).

[19] ICRC position on autonomous weapon systems (*ICRC*, 12 May 2021) <https://www.icrc.org/en/document/icrc-position-autonomous-weapon-systems> accessed 14 December 2023.

[20] The point here is it depends on which definition of AWS you use. While some believe AWS are weapons of the future, some believe that they have existed in some basic form (such as anti-personnel mines) for decades.

[21] Noting the IHL principle of proportionality, codified within API does not altogether prohibit civilians harms. See e.g., Arts. 51(5)(b) and 57 API, and ICRC Customary Rule 14, available at <https://ihl-databases.icrc.org/en/customary-ihl/v1/rule14> accessed 31 October 2023.

[22] Where, if operating outside of an existing battlefield, which means that IHL would not apply, their use

T-800 'Terminator' imagined by Hollywood movie studios.[23] Perhaps one of the most controversial forms of real world AWS however, is armed swarming drones.[24]

For the purpose of this paper, the term *swarm* is taken to mean a collection of individual but identical mechanical elements (generally taking the form of non-recoverable munitions) that can act both individually and collectively.[25] While such technology is still in its infancy, robot swarms, as the name suggests, behave in a way that is synonymous with the dense collections of insects that are found in nature.[26] The focus of the following analysis is primarily legal, with the investigation seeking to demonstrate that while AWS cannot be identified as inherently unlawful (as a result of vast array of potential weapons falling under the category), IHL nevertheless prevents certain deployments. And, central to the present paper is the fact that this includes attacks that are indiscriminate in nature.[27]

On the face of it, an armed swarm might be capable of operating in adherence with Art. 48 API. Here, it is simply imagined that the swarm could manoeuvre itself through an environment where civilians were present and choose, for example, to avoid applying force to anything other than tanks.[28] Controversially, however, an armed swarm could arguably also be instructed to engage an individual, or perhaps a selection of individuals, based upon certain characteristics. A swarm might be deployed, for example, with the instruction to seek out and kill or disable all males located within a city aged between 16–55. Indeed, one opposition group has even suggested that they could be used to target individuals based upon opinions expressed on social media platforms.[29]

Perhaps unsurprisingly, some observers have demonstrated particular concern over the potential for future swarms to operate according to this latter form of instruction, regardless of the potential for it to operate in adherence with IHL.[30] This is not least

arguably violates international human rights law obligations, such as the non-derogable right to life which is codified in Art. 6 International Covenant on Civil and Political Rights (ICCPR).

23 See e.g., <https://www.imdb.com/list/ls076952805/> accessed 14 December 2023.

24 See, for example, a series of videos recorded by human rights organisations in which swarming drones are referred to as 'slaughterbots'. These can be found here, <https://www.youtube.com/watch?v=O-2tpwW0kmU> accessed 31 October 2023 and here <https://www.youtube.com/watch?v=9rDo1QxI260> accessed 31 October 2023, noting that sophisticated armed swarms such as slaughterbots are not yet thought to exist.

25 See e.g., Hambling D, 'What are Armed Swarms and Why Does Everyone Suddenly Want one?' (*Forbes*, 1 March 2021) <https://www.forbes.com/sites/davidhambling/2021/03/01/what-are-drone-swarms-and-why-does-everyone-suddenly-want-one/> accessed 21 October 2023.

26 Ibid. Note that robot swarms have also been touted as a method for tackling issues such as the decline in natural pollinators, see e.g., Willmer G, 'Robotic bees and roots offer hope of healthier environment and sufficient food' (*Horizon*, 24 February 2023) <https://tinyurl.com/yv744xr2>.

27 See, Art. 48 API (n 13).

28 The IHL principle of proportionality may of course also be relevant here (see e.g., Art. 51 (5) (b) API). For present purposes, however, further analysis of this is not required.

29 See, slaughterbots (n 24).

30 See, e.g., slaughterbots (n 24). Note that under IHL, each targeting assessment must include an evaluation as to whether a human target is participating in the conflict (or whether, for example, they should be considered *hors du combat*), see e.g., Art. 41 API. Any AWS operating in conflict, therefore, must be capable of making such an assessment.

due to the fact that an armed swarm may have negative impact upon both the physical and psychological health of a civilian population, merely by way of it operating within an urban environment. This is especially pertinent given the increasing urbanisation of warfare.[31] The purpose of this paper, however, is to demonstrate that Article 51(5)(b) API is key to restricting such deployments.

To date 51(5)(b) API has been somewhat overlooked in the debate regarding swarms. Nonetheless, it is argued that if this provision is interpreted in good faith, with the ordinary meaning given to the terms contained within (as is required by Article 31 Vienna Convention on the Law of Treaties),[32] a swarm could, and arguably should, be classified a bombardment. In doing so, and by using the military decision-makers authorisation to deploy the swarm as a point of reference, many armed swarm deployments would be considered unlawful. This is due to the fact that the military decision maker can be seen to be treating a number of clearly separated and distinct military objectives as a single military objective, which in short means they would in effect be authorising an indiscriminate attack.

1. Defining Autonomous Armed Swarms

The term armed swarm could be applied to various similar, but subtly different weapons technologies. Developmental programmes such as the loyal wingman currently being tested by Boeing,[33] for example, is a swarm of sorts given that it is comprised of individual platforms. However, this can be distinguished from the subject matter of this paper because this type of system is merely a collection of combat drones. Indeed, they are even similar in appearance to remotely piloted weapons such as Predator[34] or Reaper Systems.[35]

The point here is, a system cannot be considered fully autonomous, even if it has certain autonomous features, where there is a direct link to a human operator (as is the case with the three systems identified in the previous paragraph). As previously noted, the form of swarms that is intended to be the focus of this paper are those that are, or at least

---

[31] Perhaps the most pertinent recent example being the conflict in the Gaza Strip, and area of territory 41km long and 10km wide, and home to 2.2 million people, making it one of the most densely populated areas on the planet. See, e.g., BBC World News, 'Gaza Strip in maps: Life in Gaza under siege' (*BBC News*, 8 November 2023) <https://www.bbc.co.uk/news/world-middle-east-20415675> accessed 1 November 2023. Note also that such deployments may have the effect of spreading terror among the civilian population (noting if an armed swarm deployment was authorised with the primary objective to spread terror among the civilian population the deployment would be prohibited by IHL, see in particular see, Art. 51(2) API, and ICRC Customary Rule 2, available at, <https://ihl-databases.icrc.org/en/ihl-treaties/api-1977/article-51> accessed 1 November 2023. In addition, certain deployments may arguably violate human rights obligations such as the right to liberty and security of persons as contained within Art. 9 ICCPR and, for example, Art. 5 European Convention on Human Rights (ECHR).

[32] Art. 31 Vienna Convention on the Law of Treaties, UNTS, vol. 1155, p. 33.

[33] Boeing, 'Loyal Wingman: Uncrewed but not alone' (*Boeing*, 23 November 2023) <https://www.boeing.com/features/innovation-quarterly/2021/11/boeings-loyal-wingman.page> accessed 1 November 2023.

[34] See, United States Air Force, 'Factsheet: MQ-1B Predator' <https://www.af.mil/About-Us/Fact-Sheets/Display/article/104469/mq-1b-predator/> accessed 1 November 2023.

[35] See, General Atomics Aeronautical Systems, 'MQ-9A "Reaper"' <https://www.ga-asi.com/remotely-piloted-aircraft/mq-9a> accessed 1 November 2023.

are imagined to be, comprised of a group of individual but identical elements[36] (perhaps 10's or hundreds, but theoretically thousands).[37] The elements are comparatively small,[38] but because each member is identical there is no single 'leader'. This way the swarm continues to function where individual members become inoperative.

One key benefit of this type of swarm is its adaptability. Indeed, a swarm may be used for virtually any mission. They might, for example, act as cloak, protecting a piloted aircraft by disturbing a ground-based radar detection system.[39] A swarm might also be deployed into an urban battlefield environment with each element programmed, as previously discussed, to target individuals or objects selected according to certain predefined criteria. The technology undoubtably has benefits, which is, no doubt, a driver behind swarm development,[40] and deployment.[41] However, here, it is also important to distinguish fully autonomous swarms.

There is no widespread agreement, but three terms regularly appear in the wider debate regarding AWS. These are, (i) human-in-the-loop; (ii) human-on-the-loop; and (iii) human-out of-the-loop systems. For present purposes, only an overview is of these elements is necessary. First, a human-in-the-loop system is one in which a human is involved in the decision-making process. For example, a human might identify the target (marking it with a cursor), before authorising a swarm deployment. There may be no more human involvement, however, in this case at least one human forms part of the wider weapons system.[42] A human-on-the-loop system is one which can operate independently, but where a human supervises the decision-making process. Here, the human can intervene at any time, if the system malfunctions or operates in an unexpected manner. A useful example of this is the PHALANX weapon System which has existed for decades.[43]

---

[36] See e.g., slaughterbots (n 24).

[37] See generally e.g., David Hambling, '*The US Navy wants swarms of thousands of small drones*' (24 October 2022, MIT Technology Review). Available at <https://www.technologyreview.com/2022/10/24/1062039/us-navy-swarms-of-thousands-of-small-drones/> accessed 1 November 2023. Also see, slaughterbots (n 24).

[38] Hambling, ibid. Indeed, one of the reasons swarms are both desirable and controversial, is that they have a relatively low cost and rudimentary design.

[39] See in general e.g., Claudia Conte C, Verini Supplizi S, de Alteriis G et al, 'Using Drone Swarms as a Countermeasure of Radar Detection' (2023) 20 *Journal of Aerospace Information Systems* 2.
Coco A, Dias T, and van Benthem T, 'Illegal: The SolarWinds Hack under International Law' (2022) 33(4) *European Journal of International Law* 1275.

[40] See e.g., United Kingdom Government, 'Press release: £2.5-million injection for drone swarms' (*Gov.uk*, 28 March 2019) <https://www.gov.uk/government/news/25m-injection-for-drone-swarms> accessed 1 November 2023.

[41] The Israel Defence force is believed to have deployed an armed swarm for the first time in 2021. See e.g., Hambling D, 'Israel used world's first AI-guided combat drone swarm in Gaza attacks' (*New Scientist*, 30 June 2021) <https://www.newscientist.com/article/2282656-israel-used-worlds-first-ai-guided-combat-drone-swarm-in-gaza-attacks/> accessed 7 November 2023.

[42] See e.g., 'Javelin' (*Lockheed Martin*) <https://www.lockheedmartin.com/en-us/products/javelin.html> accessed 1 November 2023.

[43] Raytheon, 'Phalanx Weapon System' (*Raytheon*) <https://tinyurl.com/2mj53kb4> accessed 1 November 2023.

To be considered fully autonomous, a weapon should be capable of carrying out the entire decision-making loop, including, for example, target identification. These are referred to as human-out of-the-loop systems. There is some debate as to whether out-of-the-loop weapons systems exist, though arguably, some loitering munitions could be categorised as such.[44] Even here though, if operation is monitored by a human in any way (e.g., being recoverable via an input to abort the mission), a loitering munition would be classified a human-on-the-loop system.

While weapons development is shrouded in a veil of secrecy, most armed swarms in development, or in operation today are human-on-the-loop systems. These cannot therefore be considered fully autonomous, a human generally being involved in the decision-making process (e.g., identification of target(s), or mission). Human-out-of-the-loop armed swarms are the primary focus of this paper, though semi-autonomous swarms may still be affected if the recommendations made herein are implemented. However, it is the fully autonomous form of targeting based on characteristics that the following recommendation primarily seeks to restrict.

2. Armed Swarms and Bombardment

Given it is almost half a century since the Additional Protocols entered into force it is unlikely that its drafters imagined its rules would ever be applied to a technology that replaced human combatants. Nonetheless, AI enabled weapons, even if not yet fully autonomous, have already been deployed,[45] and more advanced systems will almost certainly follow. With that in mind, IHL must arguably be interpreted and applied, in good faith, and in such a way that accounts for such advances.

As previously noted, 51(5)(b) API is a provision that could be key to regulating the most controversial of all armed swarm deployments, i.e., those that are capable of selecting and engaging targets based upon pre-defined criteria. This obligation provides,[46]

> *Indiscriminate attacks are prohibited…[a]mong others, the following types of attacks are to be considered as indiscriminate: an attack by bombardment by any methods or means which treats as a single military objective a number of clearly separated and distinct military objectives located in a city, town, village or other area containing a similar concentration of civilians or civilian objects.*

To demonstrate how this provision should be used to limit armed swarm deployments, this remainder of this section undertakes a simple interpretive exercise. This begins by considering the ordinary meaning of the term 'bombardment', which is the primary focus for this paper. Here, if asked to imagine an act of bombardment, one might be drawn to the carpet-bombing tactics used by the Allied and Nazi forces during

---

[44] See, Rheinmetall, Hero Loitering Munitions. Here Rheinmetall identify that 'the term loitering munition… is derived from the munition's ability to remain undetected in the airspace above the target area for an extended period of time and to strike when the right moment arrives.' See, 'Hero Loitering Munitions' (*Rheinmetall*) <https://www.rheinmetall.com/en/products/loitering-ammunition/loitering-munitions-hero> accessed 1 November 2023.

[45] Loitering munitions being an obvious example.

[46] When read in conjunction with Art. 51(4) API.

the second world war. Indeed, this appears to be the type of behaviour the drafters of the additional protocols were seeking to prevent.[47] Nonetheless, bombardment is simply defined as 'a continuous attack with either bombs, shells, or other missiles.'[48]

With that in mind, if swarms are capable of being defined as a bombardment two simple questions must be answered in the positive. The first question regards the matter of whether once deployed, a swarm operates in a continuous manner, and two, whether the individual elements of a swarm constitute a bomb, shell, or other missile. In the first instance, 'continuous' is subsequently defined as 'forming an unbroken whole; without interruption: *the whole performance is enacted in one continuous movement*.'[49] Here, one could argue that a swarm may not necessarily apply force in a continuous manner. Nonetheless. it is argued that a swarm does operate *continuously* from the moment at which a decision-maker authorises it deployment, to the later moment in time where it either completes its mission or for some other reason ceases to operate. In other words, it operates in a continuous manner.

The second issue is connected to the application of force, the issue here being the matter of whether a swarm constitutes a continuous attack with either a bomb, shell, or other missile. It is argued that this is the only logical definition – with the elements of a swarm already having been referred to as a munition. The U.S. Department of Defence (DoD) defines a munition as a 'complete device charged with explosives; propellants; pyrotechnics; initiating composition; or chemical, biological, radiological, or nuclear material for use in operations including demolitions.'[50] For present proposes this is arguably sufficient. However, the DoD is a specialised agency, so it might also be useful to consider the the ordinary meaning of terms bomb, shell and missile.

First, a bomb is defined as 'a container filled with explosive or incendiary material, designed to explode on impact or when detonated by a timing, proximity, or remote-control device'.[51] To this, to one might reasonably add 'or autonomously', though there is no pressing need because a swarm might also be defined as a collection of *missiles*, those being defined as objects "forcibly propelled at a target either by hand or from a mechanical weapon'.[52]

It could be argued that given its autonomy, an armed swarm is not necessarily propelled by hand. However, the point here is the elements of the swarm are in themselves a mechanical weapon. In addition, if the definition of shell is utilised instead, e.g., an 'explosive artillery projectile or bomb' this minor difficulty, if there is one, is

---

47 Pilloud C, Depruex J, Sandoz Y et al, 'Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949' ICRC, (1987), para. 1946.

48 Bombardment, Oxford Dictionary of English, (OUP, Version 15.7.471). Similarly, the Cambridge Dictionary of English provides that bombardment is, a continuous attack on a place with guns or bombs, see, 'Cambridge Dictionary of English' <https://dictionary.cambridge.org/dictionary/english/bombardment> accessed 1 November 2023.

49 'Continuous', Oxford Dictionary (n 48).

50 'DOD Dictionary of Military and Associated Terms' (*U.S. Department of Defense*, November 2021) <https://irp.fas.org/doddir/dod/dictionary.pdf> accessed 15 December 2023.

51 'Bomb', Oxford Dictionary (n 48).

52 'Missile', Oxford Dictionary (n 48).

overcome.[53] Semantics aside, the key point here is that it is not particularly difficult to prove that an armed swarm operates in a continuous manner, or that the individual elements are a form of weapon to which IHL is applicable. Therefore, when the relevant terms are given their ordinary meaning a swarm can quite readily be defined as (at least a form) of bombardment.

Having demonstrated how a swarm deployment can be classified as a form of bombardment, it is still important to consider the nature of the deployment. This is because, Article 51(5)(b) does not absolutely prohibit this tactic. Instead, to be considered a violation of IHL, a bombardment must treat 'as a single military objective a number of clearly separated and distinct military objectives located in a city, town, village…'[54] Here, it is vitally important to consider the perspective of the individual authorising the drone deployment, who, simply put, will generally deploy a swarm with an instruction such as, target all males of a military age within a pre-defined area.

The point here that the decision-maker does not identifying the individual targets. Instead, they merely direct a swarm to a geographical area which is likely to contain several unidentified targets. However, this is clearly another way of stating they are treating several clearly separated and distinct military objectives, that are located in an urban environment, as a single military objective. Consequently, this form of swarm deployment must be considered a violation of Art. 51 (5)(b) API, in that the attack is conducted in an indiscriminate manner.

Conclusion

Autonomous armed swarms are at the cutting edge of weapons technology. And while they are not yet fully developed, they have the potential to significantly change battlefield operations, despite being relatively cheap to produce. Many are concerned, and perhaps somewhat justifiably, that even where civilians are not made the direct object of attack, the consequences of large-scale urban deployments may still cause great deal of civilian harms - both physical and psychological. As result, there are calls for swarm deployments to be prohibited. An issue, however, is that not all armed swarm deployments will necessarily interfere with the civilian space. Indeed, swarms cannot be demonstrated to be unlawful, per se. It is argued, therefore, that armed swarms should be regulated instead.

This paper has demonstrated that Article 51 (5)(b) API can be interpreted to account for this emerging technology, and its particularly novel way of interacting with the environment. To do this, the distinction assessment must simply be made at the point that the military decision-maker authorises a swarm deployment, as opposed to the point of the actual attack. If this is recommendation is implemented, there will be a significant number of instances where a decision-maker will have to refrain from launching an attack or else they would effectively be treating several clearly separated and distinct military objectives as a single military objective, which is prohibited by IHL.

---

[53] 'Shell', Oxford Dictionary (n 48).

[54] Article 51 (5)(b) API.

1.2 International Law Attempts to Protect Critical Infrastructures against Malicious Cyber Operations

By ***Triantafyllos Kouloufakos*** (Katholieke Universiteit Leuven)

Introduction

There was a time when the words cyber-attack had a degree of mystification on them. The early 2000s provided us with a series of cyber operations, all with increasingly serious consequences.[55] Nevertheless, twenty years ago, a cyber-attack was something worthy of news, albeit news that were not very approachable to a layman. Words like cyber worm or cyber malware were just starting to lose the fabled status that they held during the 80's and 90's, but again only just. A cyber-attack was something extremely important, something that warranted invited computer specialists in everyday news to analyze and soothe the masses that were just recovering from the Y2K scare.[56]

Today's news though, tell a different story. We have come to expect at least two or three segments of every major news site to be about a malicious cyber operation and its very serious consequence. The current conflicts in Ukraine, and very recently in Gaza, have exacerbated this. From the start of Russia's invasion, news about cyber-attacks and the opposing cyber armies, flood the news almost daily.[57] At the point of this introduction being written, the crisis in Gaza has been on for almost a week and there are already news articles about cyber operations to aid and relief groups in Gaza.[58]

It is reasonable that we have become desensitized to cyber-attacks, which is certainly dire. Offensive cyber operations become more complicated and more catastrophic by the day and unfortunately, they have been increasingly targeting critical infrastructures.[59] An energy pipeline which creates hours of car lines in gas stations,[60] a wave of attacks that

[55] Forrester N, 'A brief history of cyber-threats – from 2000 to 2020' (*Security Brief*, 12 January 2021) <https://securitybrief.co.nz/story/a-brief-history-of-cyber-threats-from-2000-to-2020> accessed 31 October 2023.

[56] Uenuma F, '20 Years Later, the Y2K Bug Seems Like a Joke–Because Those Behind the Scenes Took It Seriously' (*Time*, 30 December 2019) <https://time.com/5752129/y2k-bug-history/> accessed 31 October 2023.

[57] Starks T, 'What we've learned from a year of Russian cyberattacks in Ukraine' (*Washington Post*, 16 February 2023) <https://www.washingtonpost.com/politics /2023/02/16/what-we-learned-year-russian-cyberattacks-ukrai ne/> accessed 31 October 2023.

[58] Siddiqui Z, 'Hackers hit aid groups responding to Israel and Gaza crisis' (*Reuters*, 13 October 2023) <https://www.reuters.com/world/middle-east/hackers-hit-aid-groups-responding-israel-gaza-crisis-2023-10-13/> accessed 31 October 2023.

[59] Reed J, 'High-impact attacks on critical infrastructure climb 140%' (*Security Intelligence*, 26 June 2023) <https://securityintelligence.com/news/high-impact-attacks-on-critical-infrastructure-climb-140/> accessed 31 October 2023.

[60] Kerner SM, 'Colonial Pipeline hack explained: Everything you need to know' (*TechTarget*, 26 April 2022) <https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know> accessed 31 October 2023.

cost a city 775 million dollars only in a year,[61] a cheese distribution center which creates massive product shortages.[62] These are all recent examples of critical infrastructures being targeted by cyber-attacks and the ominous consequences that follow.

It has become apparent that regulation is urgently needed. However, international law, has lagged significantly behind in its regulation of cyber operations, specifically on critical infrastructures. While the European Union is busy creating comprehensive regulations and directives which aim on the protection of critical infrastructures,[63] international law has been debating for the first ten years whether it applies to cyberspace,[64] and when this debate ended, how it can be applied, and if it is better to first apply non-binding norms.[65] This delay has created an even bigger gap and one may argue that has given states the signal that they will go unpunished if they organize or sponsor major cyber-attacks, hidden or not behind proxies.

In this paper I submit that international law already has the tools to contribute to an effective protection of critical infrastructures against cyber operations, namely the due diligence -and by extension the no-harm- obligation, and the rule prohibiting intervention in the internal affairs of another state. I believe that these rules, with certain modifications-necessary for them to properly function in the cyber environment-can be important legal protections against cyber-attacks, by threatening legal repercussions both to aggressor and to negligent states who allow their systems to be used for such malicious purposes.

Starting with due diligence and no-harm, I will give a brief recount of their origin and position within international law and I will underline their flexibility as international legal rules. Furthermore, I will consider the difficulties that they may face when applied to cyberspace and finally analyze how certain elements of the rules may be modified in order to apply to cyberspace. Subsequently, I will turn to the non-intervention principle analyzing its origins and its elements. Moreover, I will reflect on how these elements function in the cyber domain and whether they should be tweaked towards an effective application of the rule.

---

61 Fox-Sowell S, 'New York lost $775M in cyberattacks on critical infrastructure in 2022, report says' (*Statescoop*, 10 October 2023) <https://statescoop.com/new-york-775-million-cyberattacks-critical-infrastructure/> accessed 31 October 2023.

62 Maruf R, 'The surprising reason you can't find cream cheese anywhere' (*CNN Business*, 18 December 2021) <https://edition.cnn.com/2021/12/18/business/cream-cheese-cyberattack-schreiber-foods/index.html> accessed 31 October 2023.

63 See for example Regulation (EU) 2019/881, OJ L 151, European Parliament and Council, 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) OJ L 151; Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union [2022] OJ L333/80, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) OJ L 333.

64 UNGA, 'Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security', UN Doc. A/68/98, para 19 (2013).

65 UNGA, 'Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security', UN Doc. A/70/174, para 24 (2015).

1. The no-harm- due diligence duo: A rule(s) for all seasons?

The obligation to prevent transboundary harm (alternatively the no-harm principle) has been formulated in the *Trail Smelter Arbitration*[66] and was considered customary international law by the International Court of Justice (ICJ) in the *Corfu Channel* case[67], a conclusion which has been reaffirmed in the *Pulp Mills* and the *Certain Activities in the Border Area* cases.[68] According to said principle, States have an obligation to prevent the use of their territory for activities causing injury or damage in the territory of another State as well as a duty to prevent transboundary harm from hazardous activities. It is considered a core part of international environmental law and of its many regimes (e.g. the law of international watercourses)[69] and has been developed extensively within this context.

Due diligence is a very old concept in international law referred to in very old and very recent arbitral awards,[70] and in decisions of international tribunals, namely the ICJ[71] and the International Tribunal on the Law of the Sea (ITLOS)[72] and has been accepted as a general principle of law.[73] There are many scholarly debates as to the nature and even the definition of due diligence as it has been called a "duty", "obligation" "principle" and "rule", thus creating wide doctrinal confusion.[74] Developing a commonly accepted definition of due diligence is beyond the scope of this paper. Nevertheless, for working reasons I will adopt that due diligence works through introducing positive obligations upon states to prevent unlawful situations and it can function both as a primary and a secondary international law rule.

In the context of this paper, I submit that the no-harm principle, and the due diligence obligations it creates, can be applied to cyberspace. This application would

---

66 *Trail Smelter Case (United States of America v. Canada)* Judgment (1938, 1941) 3 RIAA 1905 ICJ Rep 29.

67 *ICJ, Corfu Channel (United Kingdom of Great Britain and Northern Ireland v Albania)* Judgment [1949] ICJ Rep 4.

68 *ICJ Pulp Mills on the River Uruguay (Argentina v Uruguay)* Judgment [2010] ICJ Rep 2010, p. 14; ICJ, *Certain Activities Carried Out by Nicaragua in the Border Area (Costa Rica v. Nicaragua) and Construction of a Road in Costa Rica along the San Juan River (Nicaragua v. Costa Rica)* Merits, Judgment [2015] ICJ Rep 2015.

69 Susane Schmeier and Joyeeta Gupta, 'The principle of no significant harm in international water law' (2020) 20 *International Environmental Agreements: Politics, Law and Economics* 597.

70 *Youmans (U.S.) v. United Mexican States, 4 R.I.A.A. 110, 116 (Gen. Cl. Comm'n 1926)*; Permanent Court of Arbitration, *PCA, South China Sea Arbitration, Philippines v. China, Award of 12 July 2016, PCA Case No 2013-19,* ICGJ 495, para 744.

71 *Corfu Channel Case* (n 13) p. 22; *ICJ Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro)*, Judgment [2007] ICJ Rep 43; Pulp Mills Case (n 68), paras 101, 197 and 204.

72 ITLOS Seabed Disputes Chamber, *Responsibilities and Obligations of States Sponsoring Persons and Entities with Respect to Activities in the Area*, Advisory Opinion [2011] ITLOS Reports 2011, paras 110–112, 117–120, 131–132; ITLOS, *Request for an Advisory Opinion Submitted by the Sub-Regional Fisheries Commission* (*SRFC*), Advisory Opinion [2015] ITLOS Reports 2015, paras 125–132, 146–150.

73 Joanna Kulesza, *Due Diligence in International Law* (Brill 2016), p. 19.

74 Peters A, Krieger H and Kreuzer L 'Due Diligence in the International Legal Order Dissecting the Leitmotif of Current Accountability Debates' Peters A, Krieger H, Kreuzer L (eds), *Due Diligence in the International Legal Order* (OUP, 2020); Brunnée J, 'Procedure and Substance in International Environmental Law' (2020) 405 *Hague Academy Collected Courses* 70.

create obligations for states to take measures to prevent that their computer systems are not used to conduct a malicious cyber operation to another state. If a state would neglect taking such measures, this would incur its international responsibility. Accordingly, a portion of the cyber harm created by malicious cyber operations, could be redressed. Nevertheless, applying these rules to cyberspace is a challenging endeavor.

Firstly, it must be examined whether the no-harm principle can be applied beyond the regime of international environmental law. The principle may have started in such a transboundary environmental context,[75] nevertheless it has already been used in other contexts. Relevant discourse has argued that the no-harm principle can be the basis for effective climate change litigation and for enforcing obligations pertaining to climate change.[76] Furthermore, the European Union has developed its own iteration of the principle, the 'do no significant harm' principle, which is used again in relation to harm to the environment but within the context of European investment law.[77] Both of these uses indicate the malleability of the no-harm principle and how it easily interacts with different international (and not only) law regimes. Therefore, it can be considered that the no-harm principle is flexible enough as a principle in order to also apply to the cyber domain.

Regarding due diligence, the 2014 and 2016 Reports of the International Law Association (ILA) Study Group on Due Diligence in International Law mention that due diligence obligations are understood and applied differently, depending on the sector involved.[78] Nevertheless, several academics have argued that due diligence can be applied to cyberspace albeit proposing different avenues,[79] and states have expressed different opinions for applying the due diligence principle to cyberspace. [80] Until now there is no uniform opinion about the way that due diligence may apply to cyberspace. However, for the purposes of this paper, and since the no-harm rule is the main focus of this paper, it is submitted that obligations of a due diligence nature can be applied and function in cyberspace in the same way that they apply to the non-cyber domain.

---

75 *Trail Smelter* (n 66); *Corfu Channel Case* (n 67).

76 Nedeski N, Sparks T, and Hernandez GI, 'The World Is Burning, Urgently And Irreparably: A Plea for Interim Protection against Climatic Change at the ICJ' (2023) 22(2) *The Law & Practice of International Courts and Tribunals* 301; Maljean-Dubois S, 'The No-Harm Principle and the Foundation of International Climate Change Law' in Benoit Mayer and Alexander Zahar (eds) *Debating Climate Law* (CUP, 2021), pp. 15–20.

77 Karageorgou V, 'The Environmental Integration Principle in EU Law: Normative Content and Function also in Light of New Developments, such as the European Green Deal' (2023) 8(1) *European Papers* 159.

78 ILA, 'Study Group on Due Diligence in International Law', First Report, (2014); ILA, 'Study Group on Due Diligence in International Law', Second Report (2016).

79 Schmitt M, 'In Defense of Due Diligence in Cyberspace' (2015-2016) 125 *The Yale Law Journal Forum* 68; Efrony D, Shany Y, 'A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice' (2018) 112 *American Journal of International Law* 583; Talbot, E, 'Due Diligence in Cyber Activities' in Peters, A, Krieger, H, Kreuzer, L (eds), *Due Diligence in the International Legal Order* (OUP, 2020).

80 See, for example 'UNODA, 'Costa Rica's Position On The Application Of International Law In Cyberspace' (2023) <https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-(2021)/Costa_Rica-Position_Paper-_International_Law_in_Cyberspace.pdf> accessed 31 October 2023.

Since cyberspace encompasses a series of unusual characteristics as a domain (e.g. a-territoriality, almost instant transmission of information) the no-harm principle cannot be applied as is. However, this does not mean that it is inapplicable. If certain elements of the principle are slightly modified, it is my contention that it can apply to cyberspace and be used to effectively redress cyber harm. In this paper, I will address two of those elements, the type of harm and the standard of knowledge required.

The first obstacle that must be surpassed, is the type of harm needed, in order for the no-harm principle to apply to cyberspace. It has been questioned, whether the no-harm principle can apply to types of harm that are beyond the environmental realm, to cover harms not related to the ecology.[81] Furthermore, it has also been questioned whether the no-harm principle can also cover non-physical harm.[82] Since the harm of cyber operations is mostly intangible and it is often not related to the environment, both of those questions are relevant for the application of the no-harm principle to cyberspace.

For the first part of the obstacle, there is enough evidence to support that the no-harm principle may cover harms beyond an ecological or environmental context. The International Law Commission (ILC), in its Draft Articles on Prevention of Transboundary Harm from Hazardous Activities defines harm as 'harm caused to persons, property and the environment'.[83] This position is also supported by judicial practice. When the *Trail Smelter* Arbitral Tribunal was looking at the history of the principle it found that the obligation not to cause transboundary harm includes any 'injurious acts to the territory of another state, persons or property therein.[84]

The second obstacle is slightly more difficult to overcome, especially considering that when the ILC started drafting the Draft Articles on Prevention of Transboundary Harm, it consciously chose to focus only on physical harm.[85] However, this decision was a practical one, that recognized the absence of state practice on the matter, when the discussion for the articles was current (1983) and thus making ILC's work easier.[86] Nevertheless, there is evidence that states considered transboundary non-material injuries, even before 1983. Existing state practice, mainly in the field of radio-telecommunications, indicates that since 1927 states have agreed to refrain from and prevent harm that has no physical consequences.[87] Since states recognized duties to prevent such types of non-physical harm since 1927, and absent contrary state practice

---

81 Dias T, Coco A, *Cyber Due Diligence in International Law* (Oxford Institute for Ethics Law and Armed Conflict, 2021), p. 139.

82 Duvic-Paoli, L-A, *The Prevention Principle in International Environmental Law* (CUP, 2018), 181.

83 Article 2(b) ILC, 'Draft Articles on Prevention of Transboundary Harm from Hazardous Activities', ILC Yearbook 2001/II(2).

84 *Trail Smelter* (n 66) 1963.

85 ILC, Draft Articles on Prevention (n 83) 151.

86 Ibid.

87 ITU, 'Constitution and Convention of the International Telecommunication Union (with annexes and optional protocol)', (adopted on 22 December 1992, entered into force 1 July 1994), 1825 UNTS 31251; ILC, 'Survey of State practice relevant to international liability for injurious consequences arising out of acts not prohibited by international law, prepared by the Secretariat', UN Doc A/CN.4/384, (1984), paras 58, 115.

and *opinio juris*, it can be argued that the no-harm principle can encompass cases of non-physical harm and thus apply to cyber operations.

The second obstacle that must be surpassed, in order for the no-harm principle to be applied to cyberspace, is connected to the standard of knowledge requirement. Normally, the no-harm principle is triggered by actual or constructive knowledge of even remote risk and excludes unforeseen harms.[88] However, the element of constructive knowledge has not been clarified when applied to cyberspace. Furthermore, this standard presupposes that states should proactively, constantly, and vigilantly monitor their networks in relation to the gravity of the harm.[89] Thus, an application of the no-harm principle to cyberspace would oblige states to monitor continuously and be vigilant in their use of Information and Communication Technologies (ICTs).

The claim that such an obligation to monitor networks exists now in international law is tenuous at best, as states' opinions on the issue, as well as the relevant scholarly discourse are divided. There are scholars who advocate that a duty of state to monitor its networks exist in different degrees. Indicatively, there are opinions that consider such a duty a prerequisite of constructive knowledge,[90] others that also support a duty to react,[91] and even some that call for 'proactive measures of vigilance and monitoring.'[92] On the other side of the fence, there are scholars that consider that such a duty to monitor could easily invite human rights violations from oppressive (and not only) regimes[93] while others outright reject the existence of such a duty.[94]

In my opinion, a state's duty to monitor its networks can exist in the contest of applying the no-harm principle to cyberspace. The existence of such a duty would not cancel all the other obligations of the states, especially its human rights obligations which would continue to co-exist with a due diligence duty to monitor. The fear that states will overreach and violate international law, should not be a reason that we refuse to apply an international law rule. I would not go as far as to say that states should also have a duty to react, but international law is not foreign to duties to monitor as many regimes include such duties (e.g. the law of nuclear disarmament).[95]

To conclude, I believe that the no-harm principle has the potential to act as a deterrent to major cyber-attacks, especially against critical infrastructures. From an international law standpoint, there is nothing that prevents its application to cyberspace. If states know that they will be responsible for being negligent regarding harmful

---

88 Couzigou, I, 'Securing Cyber Space: The Obligation of States to Prevent Harmful International Cyber Operations' (2018) 32 *International Review of Law, Computers & Technology* 37.

89 ILC, Draft Articles on Prevention (n 83).

90 Buchan, R, 'Cyberspace, Non-State Actors and the Obligation to Prevent Transboundary Harm' (2016) 21(3) *Journal of Conflict & Security Law* 429.

91 Bannelier-Christakis K, 'Cyber Diligence: A Low-Intensity Due Diligence Principle for Low-Intensity Cyber Operations?' (2015) 14(1) *Baltic Yearbook of International Law* 23.

92 Talita Dias and Antonio Coco (n 81).

93 Talbot (n 79).

94 Delerue F, *Cyber Operations and International Law* (CUP, 2020), p. 360.

95 Takano A, 'Due Diligence Obligations and Transboundary Environmental Harm: Cybersecurity Applications' (2018) 7(4) *Laws* 36.

cyber operations, they will have a motive to increase their cybersecurity standards, introduce new cybersecurity protections, and generally be more vigilant against cyber-attacks. And lastly, taking into account that the most vulnerable targets tend to be their critical infrastructures, states will rush to fortify them fostering thus a new culture for cybersecurity.

2. The non-intervention principle: A classic rule for a modern solution

The non-intervention principle is one of the fundamental principles of international law.[96] Based on sovereign equality and political independence,[97] it forbids states from intervening coercively in the domestic or foreign affairs of other states.[98] Its importance in international law has been recognized both by the Permanent Court of International Justice (PCIJ)[99] and by the ICJ.[100] According to the latter, non-intervention represents 'the right of every sovereign State to conduct its affairs without outside interference and is one bearing on matters in which each State is permitted, by the principle of State sovereignty, to decide freely'.[101]

However, cyberspace alters the playing field significantly. Newfound threats like digital election interference[102] and the increase of state sponsored cyber-attacks aiming to intervene to other states' internal affairs[103] disrupt significantly the two constitutive elements of intervention, namely the element of coercion and the element of *domaine réservé,* when applied two cyberspace, as they are applied in a kinetic context. Thus, like the case of the no-harm principle, it must be examined whether those two elements need to be modified in order to apply in a cyber context.

The first element that I will consider is the element of coercion. There is an abundance of sources which establish the stalwart link between non-intervention and coercion, which includes judicial practice,[104] state practice,[105]and even scholarly views about its existence in a cyber context.[106] It is thus accepted that for an intervention to be prohibited, coercion is essential. The threshold of coercion, however, can still be

---

96 ICJ, *Case Concerning Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America),* Judgment [1986] ICJ Rep 1986, para 202.

97 Jennings R and Watts A, *Oppenheim's International Law. Intervention*, 1 (OUP, 2008), pp. 430–49.

98 UNGA, 'Declaration on Principles of International Law concerning Friendly Relations and Cooperation among States in accordance with the Charter of the United Nations', UN Doc. A/RES/2625(XXV) (1970).

99 PCIJ *S.S. Lotus (France v. Turkey)* Judgment [1927] PCIJ (Ser. A) No. 10, 18.

100 *Corfu Channel Case* (n 67), 35; *Nicaragua Case* (n 96), paras 202, 205, 25; *Armed Activities on the Territory of the Congo (Dem. Rep. Congo v. Uganda)*, Judgment [2005] ICJ Rep 168, paras 161–165

101 *Nicaragua Case* (n 96), para 205.

102 Tsagourias N, 'Electoral cyber interference, self-determination and the principle of non-intervention' (EJIL: *Talk!*, 6 August 2019) <https:// www .ejiltalk .org/ electoral -cyber -interference -self -determination -and -the -principle -of -non -intervention -in -cyberspace/> accessed 31 October 2023.

103 Hathaway O et al, 'The Law of Cyber-Attack' (2012) 100 *California Law Review* 817.

104 *Nicaragua Case* (n 96), para 205; *Corfu Channel Case* (n 67), para 35.

105 Friendly Relations Declaration (n 98).

106 Schmitt M, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (CUP, 2017), Rule 66.

considered elusive as there are different opinions about it.[107] The opinions converge however that coercion removes from a state its control over its sovereign will. In the cyber age, these ideas of coercion create some difficult challenges. For example, what is the required magnitude of coercion? Is absolute loss of control required, or can it be partial? What if an initial act of influence or interference sets in motion a series of circumstances that deprives the victim State of authority over a particular matter?

The cyber environment makes it increasingly difficult for coercion to be proven. Cyber interventions are usually more nuanced and, in the end, fail to reach the threshold of the 'traditional' iteration of coercion. This leads to often catastrophic cyber-attacks (e.g. the SolarWinds Hack) not being classified as unlawful intervention since that threshold is not met.

Considering this, there is already support by scholars that advocate for lowering said threshold[108] or reformulating it[109] in order to apply to cyberspace. An idea that exists is to interpret coercion based on the unique challenges that cyberspace presents, adopting a broad interpretation of coercion.[110] Another proposal includes looking at non-intervention through a human rights perspective and thus linking coercion with violations of different human rights elements (e.g., the right to self-determination).[111] An older approach, instructs looking not at the tools and methods when discussing coercion, but rather at the effects that this coercion has on the victim state.[112] This can prove significantly effective for cyber operations since the methods that ore often used cannot reach the traditional threshold for coercion *per se*, but their effects could. Similar to this contention, another idea proposed that instead of coercion, the focus should be whether an activity causes a disruption, in order to amount to an unlawful intervention.[113] This also seems to be a good fit for cyber intervention, especially considering cases of disinformation, news manipulation and propaganda campaigns.

Concerning coercion, it is my submission that it can be broadened as a concept in order to apply to cyberspace. Specifically, I believe that the traditional threshold of coercion is set too high, rendering the rule prohibiting intervention useless in a cyber context. For non-intervention to be applicable in cyberspace, an effects approach, would

---

[107] Jamnejad M and Wood M, 'The Principle of Non-Intervention' (2009) 22 *Leiden Journal of International Law* 345; Kilovaty I, 'The Elephant in the Room: Coercion' (2019) 113 *American Journal of International Law Unbound* 87, p. 89; Schmitt M, '"Virtual" Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law' (2018) 19 *Chicago Journal of International Law* 30, p. 51.

[108] Schmitt M and Vihul L, 'Sovereignty in Cyberspace: Lex Lata Vel Non?' (2017) 111 *AJIL Unbound* 213.

[109] Kilovaty (n 107), p. 87; Milanovic M, 'Revisiting Coercion as an Element of Prohibited Intervention in International Law' (2023) 117(4) *American Journal of International Law* 601.

[110] Barela S, 'Cross-border cyber ops to erode legitimacy: An act of coercion' (*Just Security*, 12 January 2017) <https://www.justsecurity.org/36212/cross-border-cyber-ops-erodelegitimacy-act-coercion> accessed 31 October 2023.

[111] Tsagourias (n 102).

[112] McDougal M and Feliciano F, 'International Coercion and World Public Order: The General Principles of the Law of War' (1958) 67 *Yale Law Journal* 771, p. 782.

[113] Kilovaty I, 'Doxfare: Politically Motivated Leaks and the Future of the Norm on Non-Intervention in the Era of Waponized Information' (2018) 9 *Harv. Nat'l Sec. J.* 146, p. 169 *et seq*; Kilovaty I, 'The international law of cyber intervention' in Nicholas Tsagourias and Russel Buchan (eds) *Research Handbook on International Law and Cyberspace* (EE, 2nd edn, 2021), p. 112.

be better suited, especially taking into account the plurality and the variety of cyber threats. In any event, following effects-based approaches to apply international law rules to cyberspace, has already proven useful, since such an effects-based approach is one of the most dominant when applying the prohibition to use force in cyberspace.[114]

The second element to be considered is the one of *domaine réservé*. In *Nicaragua,* the ICJ defined the *domaine réservé,* as 'matters in which each State is permitted, by the principle of State sovereignty, to decide freely'.[115] The Court also provided two very broad examples 'the choice of a political, economic, social and cultural system, and the formulation of foreign policy'.[116] Michael Schmitt made an effort to distinguish between issues that fall under the exclusive jurisdiction of the State and those that do not. Schmitt says that while 'commercial activities typically do not,' 'elections fall within the *domaine* réservé.'At first glance, if a State participated in a meddling act 'meant to give business advantages to its national companies' it wouldn›t violate the non-intervention tenet.[117] Nevertheless, Schmitt also acknowledges that there may be a grey zone in the context of online communications.[118]

Furthermore, as was the case with coercion, cyberspace blurs the line regarding what can be considered as *domaine réservé* of a state. For example, would the dissemination of disinformation on a private social media site be considered an interference with the electoral system? Is targeting consumers with false news about their elected authorities considered political interference? Given that private internet players such as Facebook and Twitter serve no sovereign purpose, it appears contradictory to regard any behavior occurring on these platforms as *domaine réservé*.[119] In addition, the growing presence of non-state actors, which may have tenuous connection with states-not enough for attribution to be established-complicates things and questions the character of non-intervention as solely an inter-state rule.

Thus, the element of *domaine réservé* must also be tweaked in order to properly apply to cyberspace. There have already been some proposals on the matter. To illustrate, it has been suggested that *domaine réservé* must be reinterpreted as *domaine privilégié*. This notion, based on the protective (or territoriality) principle,[120] would include the traditional elements of *domaine réservé* along with a state's vital interests (e.g. national security and public safety) which are 'necessary for the very survival of a state but also those that are essential for its independence, autonomy and stability'.[121] Others have supported that if the actualised harm of an attack forces a state to make a policy change

---

[114] Buchan R, 'Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?' (2012) 17 *Journal of Conflict and Security Law* 211, p. 212; Dinniss H H, *Cyber Warfare and the Laws of War* (CUP, 2012), p. 74.

[115] *Nicaragua Case* (n 96), para 205.

[116] Ibid.

[117] Schmitt M, 'Grey Zones in the International Law of Cyberspace' (2017) 42 *Yale Journal of International Law* 1.

[118] Ibid.

[119] Kilovaty, 'The international law of cyber intervention' (n 107), p. 103.

[120] Higgins R, *Themes and Theories*, (OUP, 2009), pp. 799–810.

[121] Moulin T, 'Reviving the Principle of Non-Intervention in Cyberspace: The Path Forward' (2020) 25(3) *Journal of Conflict & Security Law*, p. 437.

that it would not have made without the existence of said attack, even if the harm was not done in a sector covered by the *domaine réservé,* this attack is considered prohibited intervention.[122]

As with coercion, the latter of the aforementioned contentions, which is based on an effects approach, seems to be the best fit for cyberspace particularities. This would allow the rule to be applied despite the quiet restrictive traditional iteration of *domaine réservé* and also take into account the blurring of the lines between state and private that cyberspace inevitably imposes.

Conclusion

Reflecting on the analyzed elements of traditional international law rules, we can draw some conclusions on how said rules may be applied to cyberspace. First and foremost, I believe that the aforementioned analysis is proof that international law may be tweaked in order to address situations in the field of cyberspace, even though the specific international law rule was not created to apply to that specific situation. International law has shown throughout the years that it can be flexible and its rules be modified according to the particular context they are applied. Any calls to the opposite, only contribute to the rigidity and sluggishness for which international law is infamous for.

Secondly, due to its peculiarities, cyberspace seems to favour a version of the rules that focuses on an effects-based approach. Due to the rapid speed with which cyber-attacks are conducted, the possibility to use multiple proxies, as well as the ease with which the instruments of the attacks are obfuscated, it is better to focus on the damage that the cyber-attack has caused that the action itself. This is not the perfect way, but it is the pragmatic way to effectively regulate, even in part, cyberspace. This concerns both the application of the no-harm principle and the principle of non-intervention when applied to cyberspace.

The protection of critical infrastructures against malicious cyber operations is an issue of vital importance and it has not been given the attention it deserves. International law can play a considerable part and it only needs to utilise some of its most traditional and basic rules. The due diligence obligations of the no-harm principle, and the prohibition of intervention are cornerstones of the international legal order. Nevertheless, this exercise can also function as a way to underline the need for flexibility when applying international law and the importance of attempting to apply the existing rules before starting to create new ones.

[122] Coco A, Dias T and van Benthem T, 'Illegal: The SolarWinds Hack under International Law' (2022) 33(4) *European Journal of International Law* 1275, p. 1281.

CHAPTER II

INTERNATIONAL JUSTICE

2.1 Digital Transformation and Access to Justice

By ***Mohamed Gomaa*** (University of Hamburg)

Introduction

„Justice delayed is justice denied“[123]

In a world where we are used to interacting with our banks anytime, anywhere and on any device, and where we can order from Amazon and receive the goods the next day, many citizens are frustrated with the current interaction model with the government, particularly in the justice sector. Moreover, existing justice institutions find it difficult to cope with the demands for justice.

Many courts and other judicial bodies still rely on in-person and manual paper-based trials, which are vulnerable to manipulation and deterioration. Therefore, the need to bring fundamental shifts in the way institutions deliver justice has been acknowledged for some time now.

Several attempts in France to transform into a so-called "digital republic" have been adopted. A law project has submitted by the National Digital Council (CNN) on such issue in June 2015, resulted in the law no. 2016-1321 of 7th October 2016, regarding a "Digital Republic" that aimed at supporting digital transformation in all sectors of the country which constitutes a basic work that only needs to be enriched.[124]

Moreover, the COVID-19 pandemic is putting unprecedented pressure on justice infrastructure, resulting in trials being postponed and services being suspended. What if the current health crisis was an opportunity to rethink the justice system to adapt to the digital age? Find out how circumstances are leading the way in the DT of justice as a facet of the UN 2030 Sustainable Development Goals.[125]

This research is interested in analyzing the changes that technology "digitalization" generates in the judicial sector, mainly focusing on Courts' outputs, how it could facilitate access to justice as well as its limits and possible dangers.

Generally, preserving the principles of the rule of law remains a major concern. The insert of DT should help maintain and enhance the quality of how the judiciary is exercised. In other words, legal disputes must continue to be resolved in fair and independent procedures.

---

[123] William Ewart Gladstone is a British statesman and Liberal politician. in a career lasting over 60 years, he served for 12 years as Prime Minister of the United Kingdom, spread over four terms beginning in 1868 and ending in 1894. He also served as Chancellor of the Exchequer four times, serving over 12 years.

[124] LOI n° 2016-1321 du 7 octobre 2016 pour une République numérique <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000033202746/>.

[125] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee, and the Committee of the Regions <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0710>.

This paper participates in the success of DT projects in judicial systems as a reform tool undertaken by governments, local and international bodies working in the field supporting modernization for justice infrastructure in developing countries and countries under-development. It shows the effects of such digitization on the efficiency of courts' output and access to justice. It also enhances the existing literature on DT in judicial services since it is rare. The paper mainly answers the following question, Does the digital transformation (DT) affect the access to justice?

Theory and Literature

Once following the literature, we found that the performance of judicial systems comprises various dimensions such as judicial independence, judicial accountability, Efficiency and judicial effectiveness.[126] In this research, we address yet another dimension of performance, namely Courts' output, accessibility to justice and how DT affects it.[127]

The UN stressed that information and communication technologies (ICT) must be used in an innovative way to ensure the achievement of the 2030 Sustainable Development Goals to promote the development of inclusive, effective and accountable institutions at all levels.[128] The transformation of the justice sector through (ICT) to digital justice results in an improvement of its efficiency, effectiveness, accountability, integrity, reliability and encouraging participation and citizen engagement.[129]

Voigt refers to numerous factors that are likely to determine the supply of court output: The number of judges per capita. In addition, their education, age, experience and so on are likely to play a role. I) the incentives that judges are subject to, in particular payment schemes and career possibilities. II) the number and quality of staff. III) the available technology. Distinguishing between factors that are immutable and those that can be influenced by policy decisions is important for being able to predict the possible success of judicial reform programs.[130]

The expected new technologies will have benefits for the judiciary and the government. Such technologies are mainly analytics, intelligent machines and security.[131]

---

[126] Voigt S and El Bialy N, 'Identifying the determinants of aggregate judicial performance: taxpayers' money well spent?' (2016) 41 *International Review of Law and Economics* 283, p. 7.

[127] Staats JL et al, 'Measuring Judicial Performance in Latin America' (2005) 47(4) *Latin American Politics and Society* 77.

[128] UN, The Sustainable Development Goals Report (2018) <https://unstats.un.org/sdgs/files/report/2018/thesustainabledevelopmentgoalsreport2018-en.pdf>.

[129] Bertot J, Estevez E, Janowski T, 'Universal and contextualized public services: Digital public service innovation framework' (2016) 33 *Government Information Quarterly* 2, p. 13.

[130] Voigt S, 'Determinants of judicial efficiency: a survey' (2016) 42(2) *European Journal of Law and Economics* 183, p. 11.

[131] Stamford C, 'Gartner's 2016, Hype Cycle for Emerging Technologies Identifies Three Key Trends That Organizations Must Track to Gain Competitive Advantage' (*Gartner*, 16 August 2016) <https://www.gartner.com/en/newsroom/press-releases/2016-08-16-gartners-2016-hype-cycle-for-emerging-technologies-identifies-three-key-trends-that-organizations-must-track-to-gain-competitive-advantage>.

The use of information and communications technology (ICT) in justice systems, including digitalization, can contribute to an increase in quality as mentioned by Warsaw Declaration II.

The impact of DT on courts attempts to map out the issues that may arise as a result of the integration of artificial intelligence (AI) into the legal system.[132]

Moreover, the DT of the judicial system provides a set of actions to monitor each proceeding individually as a key source to improvise access to justice. In other words, the progress of the case, from initiation through trial to the completion of post-disposition work, when controlled and supervised will leave no room for arbitrary or biased judgments.[133]

However, some argue widely that it is unclear whether the use of high-end technology might help in preventing and resolving the most pressing justice problems, access to justice or issues with local government about public services.[134]

Jane Donoghue talks about the development of digital justice in the courtroom, which is a little-discussed but crucial element of legal technology change. She explores the consequences of advancements in courtroom technology for fair and equitable public involvement, as well as access to justice.[135]

It can be inferred that the existing literature focuses the most on the digital government and the information technology systems in general. Additionally, numerous pieces of literature tried to measure the determinants of judicial efficiency[136], considering DT/ICT as one of them. Nevertheless, this paper is mainly focused on the DT and its effects on the court's output and access to justice.[137]

Also, the analysis of DT projects in judicial systems in numerous countries is a difficult task for lack of the available relevant data and information, take into account that the justice administration is considered critical and sensitive because it is managing critical data in civil, criminal and administrative judicial processes. This explains the difficulties faced in proceeding with observations of research approaches.

Method of Research

The article is considering the judicial service (represented in the "courts, judges, clerks,) as a production unit hands as a supplier of a certain service or product

---

[132] Zsófia F, Gyuranecz B and Krausz B, 'The impact of DT on courts' (2022) *Cybersecurity and Law* 272, pp. 272–296.

[133] Steelman DC, *Caseflow Management: The Heart of Court Management in the New Millennium* (NCSC, 2004).

[134] Kanan D, 'Use of digital technologies in judicial reform and access to justice cooperation' (*HiiL*, 2021) <https://www.hiil.org/wp-content/uploads/2021/11/HiiL-Use-of-digital-technologies-in-judicial-reform-and-access-to-justice-cooperation.pdf>.

[135] Donoghue J, 'The Rise of Digital Justice: Courtroom Technology, Public Participation and Access to Justice: The Rise of Digital Justice' (2017) 80 *Modern Law Review* 995, p. 14.

[136] Vereeck L and Mühl M, 'An Economic Theory of Court Delay' (2000) 9 *European Journal of Law and Economics* 2, pp. 243–268.

[137] 'European Commission for the Efficiency of Justice (CEPEJ) CEPEJ Studies' (*Council of Europe portal*) <https://www.coe.int/en/web/cepej>.

"judgments" from one side, and the litigants (Actors who file a case and ask for judicial services) as a demander from another side.[138]

Overall, it aims to show how the digital transformation of the judicial system could affect positively on access to justice? In other words, do countries implementing Digital transformation observe a positive effect on Access to justice or not?[139]

In this study, the data was selected based on availability (2016-2018). Also, the lack of clear and consistent data on DT/ICT has often hindered the researcher's ability to examine more data and results and affected the selection of the other different variables. This research used cross-sectional data analysis of 40 countries between 2016–2018.

1. The importance of Digital Transformation and its development

1.1 Definition of DT and its Importance

Digital Transformation (DT) is defined multiple times in literature. It is "Set of scientific methods, theories and techniques whose aim is to reproduce, by a machine, the cognitive abilities of human beings in the justice context".[140]

In such context, we could define the DT/ICT as the insertion of technology in the judicial organs in order to improve its performance, facilitate access and usage, and then achieve the efficiency and economy of justice. It could be financed by public and private sectors. **(See Figure 1)**

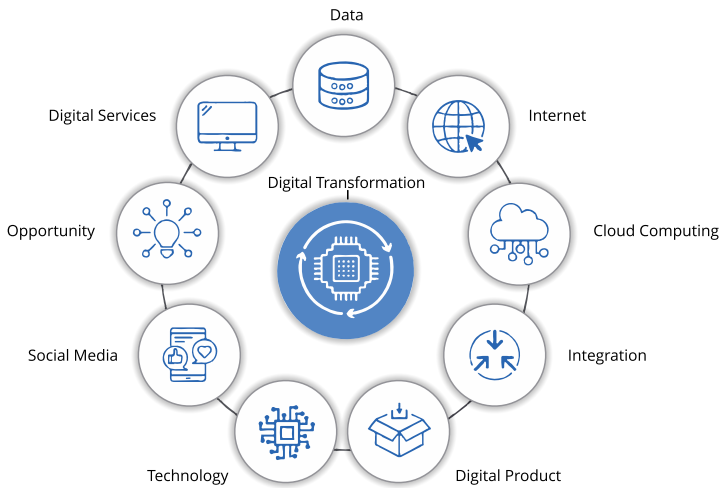


Figure 1

[138] Voigt C, Havlik D, Vogler M and Leo H, 'Crowdsourcing and Microlearning Voigt et al 2013-libre' (October 2014) <https://www.researchgate.net/publication/267528465_Crowdsourcing_and_Microlearning_Voigt_et_al_2013-libre>.

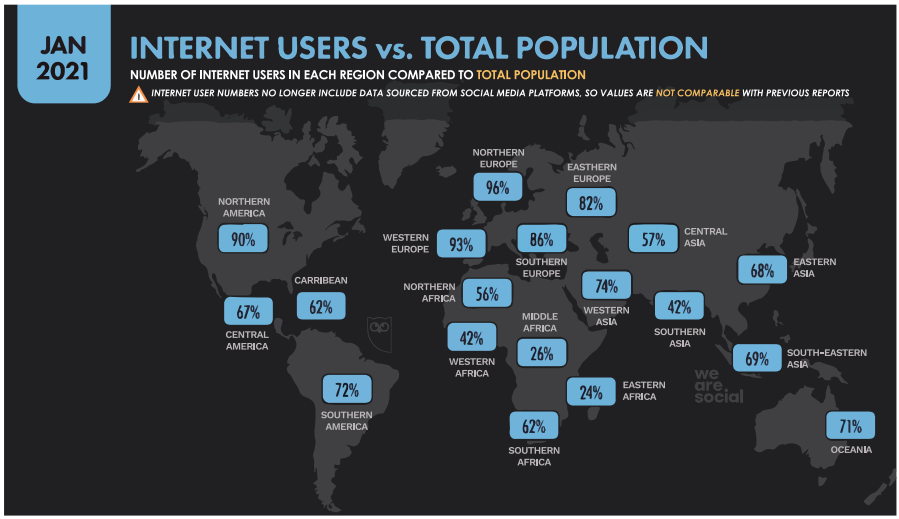
[139] Rosales V, 'Economics of Court Performance: An Empirical Analysis' (2008) 25 *Journal of Law and Economics* 231, pp. 231–251.

[140] Ibid, also See <https://rm.coe.int/cepej-2019-5final-glossaire-en-version-10-decembre-as/1680993c4c>.

We observed that those definitions agreed on two main observations that could define the DT, which are: first, DT is primarily related to entities or organizations. Second, there are remarkable differences with regard to the types of technologies[141] involved as well as the nature of the transformation taking place.[142]

There is some confusion between Digitization, Digitalization and Digital Transformation. Even if the three concepts are connected with technology, such confusion should be removed. Digitization is about how to convert from analog to digital format, while Digitalization is considering the Automation of business processes. Nevertheless, Digital Transformation is related to creating a digital sector or entity. Overall, ICT should satisfy people's needs.

Most People now are using the technology in their daily life. Therefore, ICT is not just a business issue, it is a policy issue. In fact, technology is a policy maker.



Figures 2: *The UN local government body, GSMA intelligence ITU, GWI, EUROSTAT 2021.*

Importance: The strategy of implementing DT in various spheres of public life is one of the guarantees of protecting the rights of citizens and their welfare. It is mainly used to simplify the interaction between the justice actors and facilitate accessibility, legitimacy, and legality. Numerous Countries are actively integrating this technology into their economy, industry, social and other fields.[143] Currently, we can state the onset of a new revolution in the Society, in which all areas of activity are transformed into a digital format, where the largest amount of labor and capital is spent on new innovative technologies.

[141] Horlacher A and Hess T, (2016) What Does a Chief Digital Officer Do? Managerial Tasks and Roles of a New C-Level Position in the Context of Digital Transformation. In *2016 49th Hawaii International Conference on System Sciences (HICSS)* (pp. 5126–5135). Koloa, HI, USA.

[142] Andriole 2017, Five Myths about Digital Transformation <https://sloanreview.mit.edu/article/five-myths-about-digital-transformation/>.

[143] Gaivoronskaya Y, 'Digitalization risks and threats' (2020) 8 *Advances in Law Studies* 25, pp. 25–32.

Moreover, open data of court decisions will soon become a reality in many countries. This new „black gold", that of data and knowledge, will have to be shared, once the essential condition of respecting personal data and privacy, their anonymization or pseudonymization before any publication for the general public has been mastered, while respecting national or European legislation. It is therefore essential to use this data with new tools, to compare court decisions rendered in similar cases, to allow lawyers and judges to draft arguments upon them in order to improve the quality of their respective litigation processes but also to allow States or judicial systems to reduce or encourage the reduction of unnecessary referrals to the courts, through settling repetitive disputes more quickly and at a lower cost aimed at improving the efficiency, effectiveness and economy of judicial systems.

However, the use of DT could accompany risks and some infractions regarding accessibility, privacy, Data protection and legitimacy. Always remember that in the hammer tool, the danger and the benefit are there. The hammer, which could be used to help the handyman, could also be used to kill another person. What's important here is the hand which holds it. The same is applicable to Artificial Intelligence (AI), which should neither be worshiped nor devoted to the underworld, in matters of justice. Therefore, DT requires not only technology but also how to manage such technology to reach its goals. Otherwise, it would be like putting the cart before the horse.

1.2 Development of DT

Basically, if the legal system is not a part of the socio-political structure of the State, it will be stripped of its main purpose. Humans' rights protection, through simplified administrative procedures, is the goals of modern justice and reducing its costs is the economic goal of litigation.

DT inserted in numerous conservative fields and industries including Justice. There are numerous examples of digital justice development including:

- Founding stable databases with easy and adaptive search tools.
- Create numerous platforms to cover most activities and jurisdictions of the courts.
- Successive updating of programs used in the judiciary.
- Creating various applications for Interaction with judiciary actors.
- Performing routine and repetitive work through setup auto-systems.

Currently, DT or IT equipments are available in most countries' judicial systems. Only Iceland, Albania, Serbia and Cyprus have an index lower than 3. Conversely, Spain, Austria, and Estonia stand out between 8 and 10 of equipment indices.[144]

[144] 'European judicial systems Efficiency and quality of justice CEPEJ STUDIES No. 24' (*Council of Europe portal*) <https://rm.coe.int/european-judicial-systems-efficiency-and-quality-of-justice-cepej-stud/1680788229> accessed 22 January 2022.

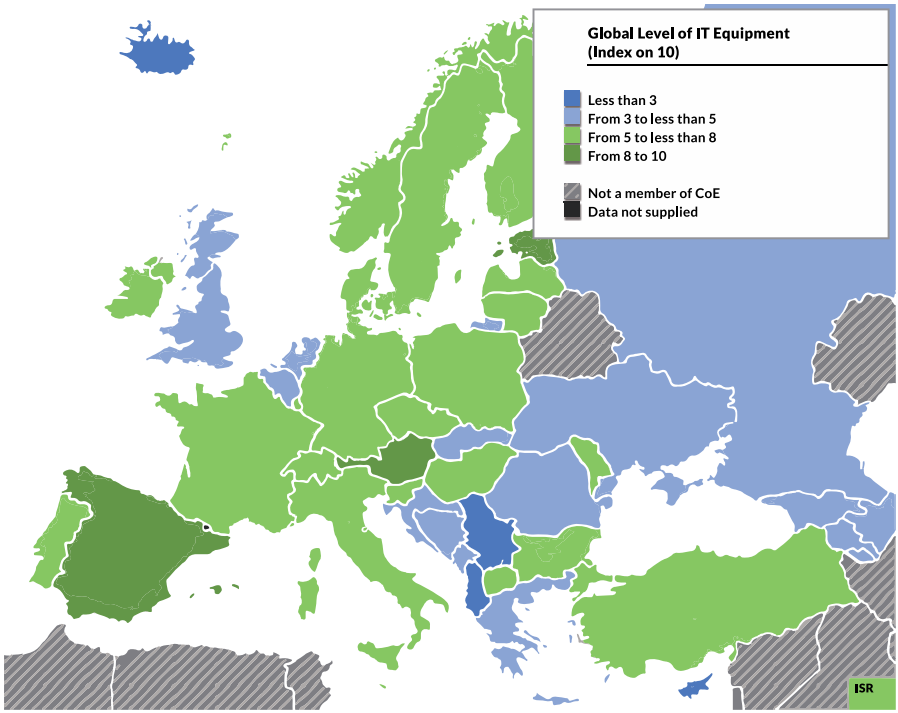


Figure 3: *Global Level of IT Equipment in Judicial Systems CEPEJ 2022*

Most governments and countries are currently seeking to create the most appropriate or favorable conditions for technology growth and a suitable environment for innovation.[145] Some researchers suggest creating a conceptual agreed model of the successful e-justice system. Other literature analyzes the steps adopted by the European Union aimed at the use of DT in the judiciary in all its potential.[146] As a set of public values, not just as a set of services, a comprehensive assessment of cyber-justice is being adopted considering the broad sense of justice.

Finally, no one can deny the importance of using quantitative analysis in the legal field.[147] It can be inferred that e-courts have their own future and it isn't so distant and very promising.

[145] Albarello F, Pianura E, Di Stefano F, Cristofaro M, Petrone A, Marchioni L, Palazzolo C, Schininà V, Nicastri E, Petrosillo N, Campioni P, Eskild P, Zumla A, Ippolito G; 'COVID 19 INMI Study Group, 2019-novel Coronavirus severe adult respiratory distress syndrome in two cases in Italy: An uncommon radiological presentation' (2020) 93 *International Journal of Infectious Diseases* 192.

[146] de Abreu MJ, 'Acts Is Acts Tautology and Theopolitical Form' (2021) 64 *Social Analysis* 42.

[147] Quattrocolo S, *Artificial Intelligence, Computational Modelling and Criminal Proceedings: A Framework for A European Legal Discussion* (Springer, 2020), p. 170.

1.3 Digital Transformation & Courts' Output & Access to justice

Article 6 (1) of **the European Convention on Human Rights** mentioned the right to a fair trial, provided that States shall set up a sufficient network of courts so that citizens can easily exercise the prerogatives they derive from this provision.

Access to justice (accès à la justice) is "All the legal and organisational factors and resources (e.g. legal aid, court fees, information) affecting the availability and effectiveness of judicial services. In the context of cyber justice, this concept includes means of accessing the law (online information on one's rights and on the status of court proceedings, publication of case law) and accessing dispute settlement procedures (online granting of legal aid, referral to a court or mediation service)".

However, some may ask to which extent the DT would affect access to justice and the rule of law? Also, how could this innovation marginalize and exclude some litigants (without technology) from accessing it?

According to the rule of law, the principles of Article 5 (the right to liberty and security guaranteed by a judge) and Article 6 of the European Convention on Human Rights (the right to a fair trial) must be protected at any time, especially during a crisis. The continuity of the functioning of the judicial system and providing its services must be ensured even in times of crisis, through alternative means such as online services or by enhancing access to information through court websites and other means of communication such as telephone, e-mail, and others.

In other words, the crisis requires an immediate and urgent response. However, any response to the crisis must be based strictly on the principles of the rule of law and the respect and protection of human rights. Emergency measures must respect the principles of legality, legal security and proportionality, and judicial oversight must be possible in a timely manner. Special attention should also be given to vulnerable groups who are likely to suffer from this situation.

2. The effect of DT on Access to Justice

In accordance with Opinion No. 14 (2011), of the **CCJE** [148]"ICT should be a tool or means to improve the administration of justice, to facilitate the user's access to the courts and to reinforce the safeguards laid down in Article (6) ECHR: access to justice, impartiality, independence of the judge, fairness and reasonable duration of proceedings" and that its introduction "in courts in Europe should not compromise the human and symbolic faces of justice".

[148] 'Consultative Council of European Judges' (*Council of Europe portal*) <https://www.coe.int/en/web/ccje> accessed 19 January 2022.

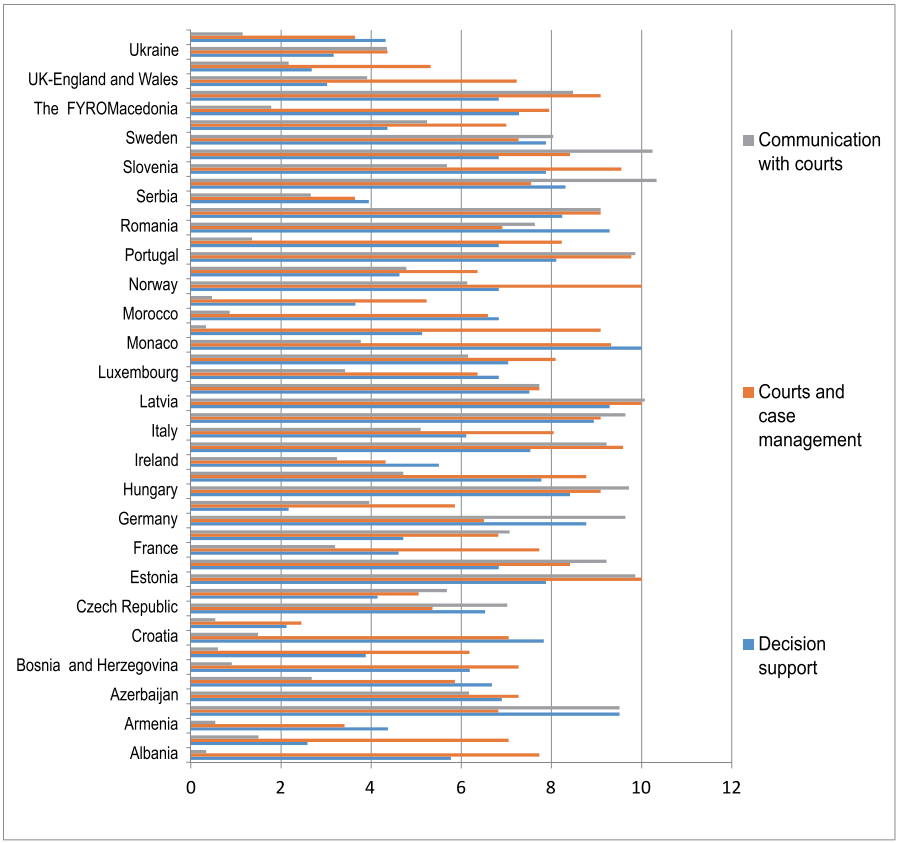


***Figure 4**: General Index of ICT in courts in 2018 "CEPEJ report 2020"*

"Access to justice is a fundamental quality-of-life issue, and our justice systems are failing people with often dire consequences".[149]

This part of the research, contrarily to the relationship of "Justice to Justice", is concerned with the relationship between the justice and citizens or users of the judicial services. It includes all platforms and applications used for the e-delivery of services to citizens, like programs, portals, online services, mobile apps, etc.

Admittedly, the existence of a sufficient number of courts, as an indispensable venue for the resolution of disputes, is one of the requirements of access to justice. However, every year, millions of people are unable to prevent or resolve their most pressing justice problems. The formal justice institutions do not adequately address their demands for justice. The Justice Needs and Satisfaction Surveys (JNS)1 conducted by HiiL in over 16 countries show on average that only 33% of people are able to

[149] Andersen E, 'Measuring the Justice Gap' (*World Justice Project*, 2019) <https://worldjusticeproject.org/sites/default/files/documents/WJP_Measuring%20the%20Justice%20Gap_final_20Jun2019.pdf> accessed 19 February 2022.

completely resolve their justice problems. 11 % are able to partially resolve them, while 31 % have an ongoing justice problem. 22 % find no resolution.[150]

Article (13) of the United Nations (UN) Convention on the Rights of Persons with Disabilities (CRPD) requires that States Parties ensure effective access to justice for persons with disabilities on an equal basis with others. (ratified by over 170 countries). Also, the Global Initiative for Inclusive Information and Communication Technologies (G3ict) – launched in December 2006 by the United Nations Global Alliance for ICT and Development, in cooperation with the Secretariat for the Convention on the Rights of Persons with Disabilities at UN DESA support the effective access to justice for persons with disabilities

Moreover, with the covid-19 effect which scaling down of justice services by justice institutions to comply with quarantines, social distancing and other public health measures and the challenge of unmet legal needs, the justice gap emerged and the situation became different. Therefore, the need for ICT/DT in courts becomes an indispensable necessity in continuing the work of judicial systems, since a low density of courts does not necessarily affect access to justice.

The accessibility of judicial systems can be evaluated along three main dimensions: informational, geographical, and financial. While the development of DT/ICT has weakened the access constraints related to the first two dimensions.[151]

Nevertheless, effective access to justice requires getting correct and sufficient information "accessibility". ICT enables citizens, regardless of their home residence and distance from the court, to lodge a legal procedure and follow the proceedings initiated. It can lower the costs, time, and travel necessary for participating in face-to-face legal proceedings and also having online files can be stored with backups and ensure paper files cannot be lost, manipulated, or ruined without a trace. However, it could not, in any event, justify the abolition of courts.

Overall, Legal and judicial issues go to the heart of people's social, economic, and physical well-being. Therefore, the use of ICT for a better understanding of people's civil legal needs and their experiences accessing justice is considered as a vital matter for designing policies that foster economic development and inclusive growth according to the UN's Sustainable Development Goals (SDGs). In this part, the paper handles the effect of DT/ICT on the access to justice in civil and commercial courts, then Administrative courts and criminal courts. This covers about 40 countries between the period 2016 and 2018 by over-viewing the incoming cases as an indicator of access to justice.[152]

---

[150] Kanan D, 'Use of digital technologies in judicial reform and access to justice cooperation' (*HiiL*, 2021), (HiiL, 2021) <https://www.hiil.org/projects/digital-technology-and-judicial-reform/>.

[151] OECD, 'Judicial performance and its determinants: a cross-country perspective, A GOING FOR GROWTH REPORT No. 05' (2013) <https://read.oecd-ilibrary.org/economics/judicial-performance-and-its-determinants_5k44x00md5g8-en#page1>.

[152] See, <https://public.tableau.com/app/profile/cepej/viz/CEPEJ-Variationsv2020_1_0EN/Tables>.

2.1 Incoming Cases before Civil and Commercial Courts

Other recent research by the World Justice Project underscores the magnitude of the global problem. According to WJP's recent report[153] 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.

Vulnerable groups, (including low-income populations, recipients of government benefits, and the unemployed), are affected disproportionately, they are more likely to have legal problems and to experience hardship as a result of their legal problems.

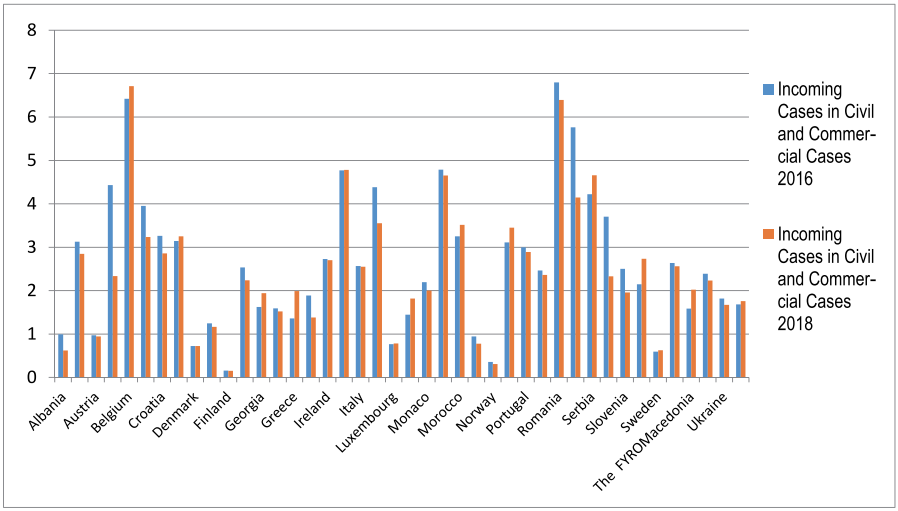


Figure 5: *Incoming cases in the first instance civil and commercial Courts (2016–2018), Source: (**Stata CEPEJ**).*

Figure (5) refers to the number of incoming first instance civil and commercial litigious cases per 100 inhabitants in 2016-2018. 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.

The differences between States and entities are considerable. The lowest value has been recorded in Finland (0.1) and the highest in Belgium (6.7) per 100 inhabitants. While, there is an observable reduction from 4.4 to 4.2 of incoming cases in Azerbaijan.

Overall, there are about seven 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.

[153] *World Justice Project*, p. 5.

2.2 Incoming cases before Administrative Courts

The number of incoming administrative cases per 100 inhabitants is typically far lower compared to other case types.

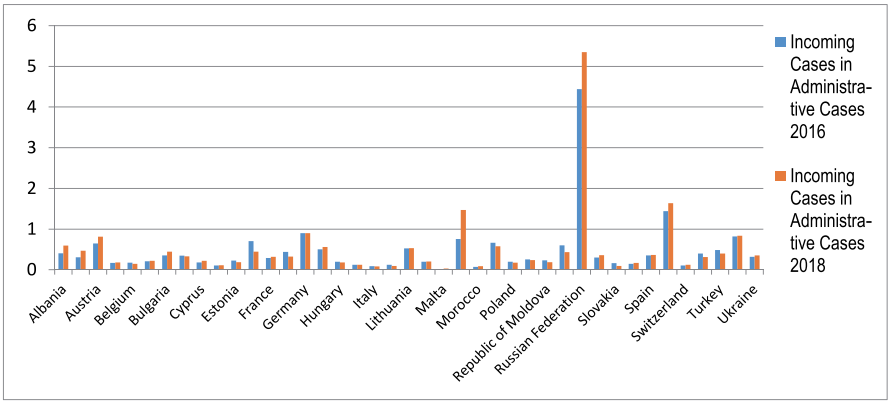


Figure 6: *Incoming cases in the first instance Administrative Courts (2016-2018), Source: (**Stata CEPEJ**).*

Figure (6) refers to the number of incoming first instance Administrative cases per 100 inhabitants in 2016-2018. The median of incoming cases in European jurisdictions is 0.3 per 100 inhabitants in (2016) and (2018), whereas the average value decreased slightly from 0.5 in the same period.[154]

Nevertheless, Montenegro, Russian Federation and Sweden recorded more than 1.0 incoming cases per 100 inhabitants. Interestingly, Montenegro and Sweden faced a significant increase compared to the previous cycle, by more than 100% in Montenegro and almost 30% in Sweden compared to 2016. Additionally, more than (7) States and entities reported from 0.5 to 1.0 received cases, while the remaining 29 received less than 0.5 administrative cases per 100 inhabitants in 2018.

2.3 Incoming Cases before Criminal Courts.

The number of incoming Criminal cases per 100 inhabitants is, contrarily to other case types e.g. Administrative, far higher.

[154] See, <https://public.tableau.com/app/profile/cepej/viz/CEPEJ-Variationsv2020_1_0EN/Tables>.

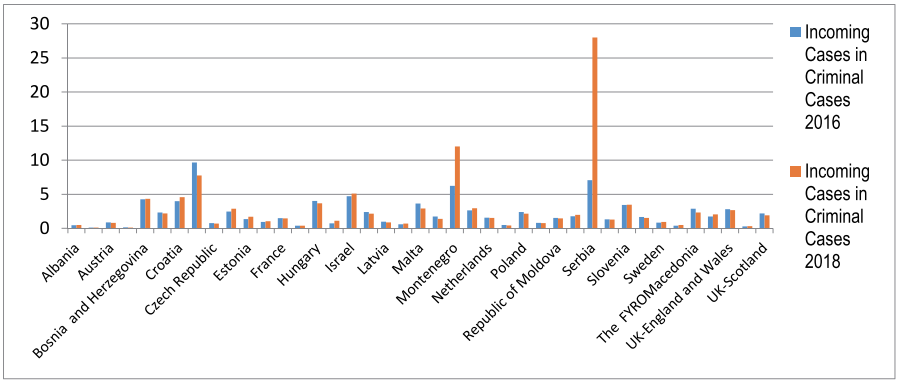


Figure 7: *Incoming cases in the first instance Criminal Courts (2016-2018), Source: (**Stata CEPEJ**).*

According to figure (7) the median of received criminal cases of first instance courts is 1.7 per 100 inhabitants in (2018), compared to 1.6 in (2016). The majority of countries and entities (more than 50%) reported from 1.0 to 5.0 received criminal cases per 100 inhabitants, while the minority ratio is below 1.0.

We find that Cyprus (7.8 cases), Israel (5.1 cases), Montenegro (12.0 cases) and Serbia (28.0 cases) reported the highest rates of incoming cases. By contrast, Armenia (0.1 cases), Azerbaijan (0.1 cases) and Ukraine (0.3 cases) have the lowest number of received cases per 100 inhabitants. Also, Serbia achieved a high jump in the incoming criminal caseload from 7.1 to 28 and Montenegro from 6.2 to 12.0.

Conclusion and Policy Recommendation

Conclusion

This research dealt, firstly, with the concept of digital transformation, the development of such concept, its importance, its relationship with other concepts and its significant influence on the rule of law. Then, the research covered and examined the impact of DT/ICT on access to justice. The research found a significant positive relationship between using DT/ICT and facilitating access to justice.

DT/ICT can achieve economies of scale. It has a positive effect on the clearance rates (CR) and facilitates access to justice. Processes can be standardised and delivered at lower costs and at higher quality. The costs of communication can be limited, thus saving travel costs and waiting times.

This preliminary finding makes it possible to identify other trends regarding the impact of DT/ICT from the perspective of efficiency and quality. It seems that the good level of development of DT/ICT tools cannot be systematically linked to a good level of court performance. Indeed, the most technologically advanced countries do not always have the best indicators for efficiency. The reason for increased (or reduced) performance is in fact to be found in the combination of several factors such as the

resources allocated, but also methods of evaluating court performance, and the use of ICT as a lever for improvement rather than as an end in itself.

Moreover, the level of DT/ICT of the courts may appear (quite logically) to depend on the Percentage of ICT in the courts' budget. However, it may be observed that it is not necessarily the States with the highest Budget or financial resources which invest most in this area. Luxembourg, for example, allocates only 1,8€ per inhabitant to computerisation, which ultimately represents only 1,3 % of the budget of the courts, and doesn't have the highest levels of efficiency & accessibility.

ICT may positively affect the efficiency of judicial systems & accessibility in a direct way. It could also indirectly, and through some other factors (like budget, judges, disposition time, training, … and others), has a positive effect on the efficiency of judicial systems.

However, ICT could also have a negative side, for example:

- The limited access and familiarity with technology also prevented certain sections of the population from participating, for example; rural, disability, marginalized, refugees, and others.
- Virtual hearings lack the empathetic environments that face-to-face hearings can create.
- Questions of identity theft & cyber crimes may arise.
- Disruptions due to poor internet connection and lack of necessary equipment also occur frequently and others.

Policy Recommendations

Digital transformation (DT/ICT) implies, in the courts, change management and user support approach. It is a new way of working, both individually (because it involves learning to work on digital files and documentation, powerful but new tools) and collectively (it is necessary to organise, structure and supervise the changes that occurred). Its success, therefore, presupposes a major investment in terms of training and management, initial and continuous, to enable magistrates and all concerned parties the appropriate use of the new tools and to promote the harmonization between the justice actors and users in all jurisdictions.

There must be a link between the work of the statistics unit that records court statistics and the tools for digital transformation, so that those data produced by the statistics unit are well studied and used in a way that achieves the efficiency of the judicial system and avoids weaknesses and shortcomings.

Moreover, DT/ICT process must promote access to justice, paying particular attention to audiences far from digital. In addition, attention to the most vulnerable litigants. It also requires the establishment of a support chain capable of providing continuous and effective assistance, including in emergencies.

Accordingly, persons with disabilities must be able to effectively participate, directly or indirectly, in all legal proceedings, including at the investigative and other preliminary stages, and in all possible roles, for example as a claimant, defendant, witness, qualified expert, juror, judge or lawyer. ex: First case before the Equality Court

in South Africa was a disability discrimination suit. Ms. Muller, a South African lawyer who uses a wheelchair 2004.

The lack of free legal aid available to persons with disabilities, here, technology can be help. EX, in the USA, Pro Bono Net, and Microsoft are developing a prototype portal that allow people to communicate naturally and receive help in a comfortable "chat" format tailored to their specific needs and abilities.

Also, it must be taken into account that in criminal trials, attendance and participation in the hearings sometimes could have a greater impact on the outcome of the case than in E-courts, by investigating the truth and better expressing the facts of the dispute mentioned in memorandums which affect on the quality of judgments issued in those disputes. For example, the judge's questioning of the accused and the witnesses in person could be more effective and have a significant impact on the progress of the case.

To succeed, Digital Justice must remain human above all. The prospect of „Digital Justice" raises numerous fears: fear that electronic exchanges will replace face-to-face exchanges (Justice without hearings), or fear that the tools of artificial intelligence replace the work of judges (predictive justice, etc.), for example. We must respond to these concerns, without depriving ourselves of interesting tools, but by reaffirming fundamental requirements, whether in terms of exchanges between trial actors, judicial work, or open data and artificial intelligence.

To conclude, the good management of the technology is a significant issue. In other words, the digital transformation (DT/ICT) of the judicial systems or the "**digital justice" shouldn't be feared, but it must be managed.**

2.2 European Production Orders and European Preservation Orders – New Instruments of Enhanced Judicial Cooperation or a Threat to Human Rights and the Rule of Law

By ***Marcin Gudajczyk*** (University of Warsaw)

Introduction

The modern world is increasingly dependent on the use of digital technologies, in particular 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 legally protected interests and to the legal system in general. This situation is particularly noticeable in judicial and prosecutorial practice. The specific nature of cybercrime means that more and more evidence of crime exists or is stored only in electronic form in IT systems. However, these systems are often under the jurisdiction of a State other than that in which the criminal proceedings take place. This, together with the need for immediate preservation of evidence, often makes it difficult or impossible to obtain evidence through traditional mutual legal assistance (MLA).

The urgent need to introduce new measures to enable judicial authorities to quickly obtain evidence through cross-border cooperation mechanisms, including direct requests to foreign digital service providers, which has been raised by criminal law doctrine and practitioners[155] has also been recognised in the fora of international organisations, which have made numerous efforts in this area. The first success in this field was the adoption of Protocol II to the Budapest Convention on Cybercrime in 2021. Considered as a strong impulse for the existing international judicial cooperation framework[156], its adoption has turned out to be only a partial success, as the regulation is still waiting to enter into force, due to the fact that, as of October 2023, only two states (Japan and Serbia) had decided to ratify it. However, the legislative activity of the European Union proved to be more effective and ended with the adoption of the Regulation of the European Parliament and of the Council on European Production Orders and European Preservation Orders (hereinafter: EPOR) on 12 July 2023.[157]

[155] See: European Union, Council of Europe and Eurojust, 'International conference on Judicial Cooperation in Cybercrime Matters' (7-8 March 2018) <https://www.coe.int/en/web/cybercrime/judicial-cooperation-in-cybercrime-matters-interna-tional-joint-conference>.

[156] Spiezia F, 'International Cooperation and Protection of Victims in Cyberspace: Welcoming Protocol II to the Budapest Convention on Cybercrime' (2022) 23(1) *ERA Forum* 101.

[157] Regulation (EU) 2023/1543, OJ L 191/118, European Parliament and Council, 12 July 2023.

1. Background

Although the need for concrete action based on a common EU approach to improve mutual legal assistance and cooperation between Member States' authorities and ISPs has been formally addressed by the European Union institutions since 2016[158] and the draft regulation was presented by the Commission as early as 2018[159], the relevant legal act wasn't adopted until June 2023. The length of the legislative process was the result of numerous comments and amendments submitted by individual Member States. The questions raised concerned various provisions, both at a general level and with regard to detailed technical and procedural issues, but mainly focused on the problem of striking a balance between the efficiency of new instruments on the one hand, and taking due account of the interests of all parties involved in their functioning on the other.[160] Once the final text of the Regulation had been agreed, it was adopted by qualified majority by the Council in a voting session on 27 June 2023[161] and published in the Official Journal of the EU on 28 July. Under its provisions, two entirely new cooperation mechanisms for enhanced judicial cooperation in criminal matters have been introduced into national legal systems, namely the European Production Order and the European Preservation Order.

2. European Production Order and European Preservation Order – General informations

The European Production Order and the European Preservation Order (hereafter referred to together as EPOs or EPdOs and EPsOs respectively) represent a completely new approach to cross-border cooperation in criminal proceedings, responding to the needs of judicial authorities in relation to the specificity of digital evidence and the need for their immediate preservation. The innovative feature of these constructions is that, unlike traditional European Investigation Orders (EIOs), which are executed through the competent authorities of the executing State, EPOs are of a direct nature. This means that, as a general rule, the competent judicial authority in the EU, when conducting criminal proceedings, including criminal investigations, or for the purpose of execution of a custodial sentence or detention order, may request any service provider offering services in the Union and established in another Member State, or, if not established, represented by a legal representative in another Member State, to produce or preserve electronic evidence, irrespective of the location of the data (Article

[158] See: Conclusions of the Council of the European Union on improving criminal justice in cyberspace, ST9579/16.

[159] Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters, COM/2018/225 final – 2018/0108 (COD).

[160] For detailed history of the adoption procedure see: https://eur-lex.europa.eu/legal-content/EN/HIS/?uri=CELEX:32023R1543.

[161] 21 Member States voted in favour of the Regulation. There were three votes against the Regulation - from Poland and Hungary, both of which objected to the proposed grounds for refusal based on Article 7 TEU procedures, but also from Finland, which pointed to the lack of balance between effective law enforcement and criminal investigation and the protection of fundamental rights. Bulgaria and Greece abstained, while Denmark did not take part in the adoption of the Regulation and is not bound by it or subject to its application.

1:1 EPOR). This provision is particularly important because, as mentioned in the preamble to the Regulation, in many cases data will no longer be stored or otherwise processed on a service provider's or user's device, but will be made available on a cloud-based infrastructure. As a result, providers of such services do not necessarily need to maintain servers in a particular jurisdiction. Indeed, some European branches of global IT companies and service providers, unwilling to cooperate with judicial and law enforcement authorities, have refused to execute EIOs on the pretext that the requested digital data is not physically located in the country to which the order is directed.[162] This excuse will no longer be accepted under the EPOR, while the application of its provisions will not depend on the actual location of the service provider's establishment or of the data processing or storage facility, as it will apply generally to all service providers offering services in the EU (Art. 2:1 EPOR). For this purpose, the term "providing services" is understood as enabling natural or legal persons in a Member State to use the ICT services[163] and having a substantial connection with the Member State, based on specific factual criteria, which is deemed to exist if the service provider has an establishment in a Member State or, in the absence of such an establishment, if there is a significant number of users in one or more member states, or if the activities are directed towards one or more member states (Art. 3:4 EPOR).

Another revolutionary aspect of EPOs is the way in which they are delivered to the addressee. In fact, the above-mentioned orders, like EIOs, are to be transmitted by means of standard forms (called "certificates"). However, unlike the EIO forms, these certificates are to be addressed directly to the designated establishment or to the legal representative designated or appointed by the service provider in digital form (Art. 9:1 EPOR), as all written communication between the competent authorities and the addressees of the orders should, as a rule, be carried out through the decentralised IT system (Art. 19:1 EPOR).

3. Conditions for issuing EPOs

Due to the different nature of the two orders, the conditions for their issuance are different. Of the investigative instruments discussed, the EPdO has the most significant consequences, as it obliges the addressee both to preserve digital evidence and to hand it over to the foreign issuing authority. As a general rule, the EPdO can only be issued if it is necessary and proportionate for the purpose of the case in question, taking into account the rights of the suspect or accused person. Furthermore, the EPdO may only be issued if a similar order could have been issued under the same conditions in a similar domestic case (Article 5:2 EPOR). It is also important to note that the admissibility of the order depends on the scope of the information requested. The electronic evidence that can be

[162] Tosza S, 'All Evidence is Equal, but Electronic Evidence is More Equal Than Any Other: The Relationship Between the European Investigation Order and the European Production Order' (2020) 11(2) *New Journal of European Criminal Law* 161.

[163] For the purposes of the EPOR, this category covers (a) electronic communications services as defined in Article 2, point (4), of Directive (EU) 2018/1972; (b) internet domain name and IP numbering services and proxy services; (c) other information society services as referred to in Article 1(1), point (b), of Directive (EU) 2015/1535 that enable their users to communicate with each other or make it possible to store or otherwise process data on behalf of the users (Art. 4:3 EPOR).

obtained through the EPO can be divided into the following categories: subscriber data, traffic data or content data (Art. 3:8 EPOR). In addition, the Regulation also refers to the category of "data requested for the sole purpose of identifying the user". This includes IP addresses and the corresponding source ports, as well as timestamps, i.e. the date and time, or the technical equivalents of these identifiers, i.e. metadata relating to the mere fact of using a network service, but not relating to specific activities. According to the Regulation, subscriber data or data requested for the sole purpose of identifying the user may be requested in all cases of criminal offences as well as for the execution of a custodial sentence or a detention order of at least four months (Art. 5:3).[164] On the other hand, the conditions for issuing an EPdO to obtain traffic or content data are more restrictive, as it is limited to proceedings for criminal offences punishable in the issuing State by a maximum penalty of at least three years' imprisonment and other offences referred to in specified EU Directives[165], if they are committed in whole or in part by means of an information system, as well as the execution of a custodial sentence or detention order of at least four months imposed for such offences (Article 5:4).

The following paragraphs of Article 5 impose further restrictions on the issuance of the EPdO. These include restrictions on data stored or processed as part of an infrastructure provided to a public authority, data protected by professional privilege and other immunities or privileges granted under the law of the executing State, or data subject to rules on the determination and limitation of criminal liability relating to freedom of the press or freedom of expression.

Unlike an EPdO, an EPsO is a decision that orders only the preservation of electronic evidence and the prevention of its removal, deletion or alteration for the purposes of a subsequent production order or request for production via EIO or MLA. It is therefore a preliminary measure which does not, at this stage, result in the transmission of the requested data to the issuing authority. The issuing of an EPsO is therefore subject to a lower degree of formal rigour. It can be issued for all offences for which it could have been issued under the same conditions in a similar domestic case, provided that it is necessary and proportionate for the purpose of the case (Art. 6:2 and 6:3 EPOR).

The scope of the information requested also determines the circle of authorities empowered to issue specific orders, in particular the EPdO. In fact, given the direct nature of the orders and the fact that they are generally not subject to prior scrutiny by the official body of the executing State, the European legislator has made the involvement of the judicial authority mandatory for certain orders. Thus, an EPdO to obtain subscriber data or data requested for the sole purpose of identifying the user may be issued by a judge, a court, an investigating judge or a public prosecutor competent in the case, or validated by them if issued by another competent authority as defined by the issuing State. However, an EPdO to obtain traffic or content data can only be issued or validated by a judge, a court or an investigating judge (Art. 4:1 and 4:2

[164] With the exception of decisions rendered *in absentia*, in cases where the person convicted absconded from justice.

[165] This includes fraud and counterfeiting of non-cash means of payment, sexual abuse and sexual exploitation of children and child pornography, attacks against information systems and terrorism-related offence.

EPOR), whereby the powers of the public prosecutor to issue an EPdO independently are limited in comparison to the EIO.

As in the area of material scope, the European legislator has opted for a less restrictive approach with regard to the group of bodies authorised to issue an EPsO. The order can be issued or confirmed by a judge, a court, an investigating judge or a public prosecutor, regardless of the type of data requested (Art. 4:3 EPOR). The Regulation also makes it possible – in emergency cases[166] – to issue any EPsO or EPdO to obtain subscriber data, or to obtain data requested for the sole purpose of identifying the user, by the non-judicial authorities without their prior validation, if this cannot be obtained in time and if these authorities could issue an order in a similar domestic case. In such cases, however, the order must be validated within 48 hours at the latest, on pain of its immediate revocation and the restriction of the use of the data obtained (Art. 4:5 EPOR).

4. Execution of EPOs

As mentioned above, the orders under discussion are to be transmitted directly to their addressees by means of certificates, namely EPOCs for European Production Orders and EPOC-PRs for European Preservation Orders, the templates for which are annexed to the Regulation. Obviously, the procedure for the execution of the orders varies according to their type and may involve the subsidiary participation of the competent authorities, including in particular a specific category of "enforcing authority" - the authority of the executing State which, according to its law, is competent to receive the orders and certificates for notification or for their enforcement in case of unjustified refusal of execution by the addressee.

The detailed EPOC enforcement procedure is set out in Art. 10 of the EPOR. It starts with the receipt of a certificate by the addressee, who must in any case immediately take the necessary measures to preserve the requested data. However, the subsequent steps depend on the nature of the data requested. Pursuant to Art. 8:1, the EPOC related to the EPdO issued to obtain traffic or content data is the subject of a notification addressed to the enforcing authority, by transmitting the certificate to this authority at the same time as to the addressee.[167] In such cases, the enforcing authority has 10 days to analyse the order and to raise one of the grounds for refusal listed in Art. 12:1 EPOR:

– the data requested are protected by immunities or privileges, or are covered by rules for the determination or limitation of criminal liability relating to freedom of the press or freedom of expression, which prevent the execution or enforcement of the order;

[166] Defined as a situation where there is an imminent threat to the life, physical integrity or safety of a person, or to a critical infrastructure, as defined in Article 2, point (a), of Directive 2008/114/EC, where the disruption or destruction of such critical infrastructure would result in an imminent threat to the life, physical integrity or safety of a person, including through serious harm to the provision of basic supplies to the population or to the exercise of the core functions of the State (Art. 3:18 EPOR).

[167] With the exception of the cases in which, at the time of issuing the order, the issuing authority has reasonable grounds to believe that the offence has been committed, is being committed or is likely to be committed in the issuing state and the person whose data are requested resides in this state.

– in exceptional cases, there are substantial grounds for believing that the execution of the order would entail a manifest breach of a relevant fundamental right as set out in Article 6 TEU and in the Charter;
– the execution of the order would be contrary to the principle of *ne bis in idem*;
– the conduct for which the order has been issued does not constitute an offence under the law of the enforcing state.

If, within 10 days of receipt of the EPOC, the enforcing authority has not raised any of the above-mentioned grounds or has already confirmed before the end of this period that it would not raise them, the addressee shall transmit the requested data directly to the issuing authority - either at the end of the 10-day period or as soon as possible, but at the latest at the end of this period. The simple 10-day deadline also applies to requests that are not subject to notification to the enforcing authority.

In emergency cases, the 10-day deadline for providing the data is reduced to only 8 hours. Where a notification is required, the enforcing authority may, at the latest within 96 hours of receipt of the notification, notify the issuing authority and the addressee of any objections or limitations on the use of the data. If the data have already been transmitted, the issuing authority shall delete them or otherwise restrict their use in accordance with the conditions specified by the enforcing authority.

The addressee shall inform the issuing authority and the enforcing authority (if notified) if it fears a possible breach of the protection rules relating to immunities, privileges and freedom of the press or of expression. The issuing authority shall then decide, on its own initiative or at the request of the enforcing authority, whether to withdraw, adapt or maintain the EPdO. The issuing authority shall also be informed of any circumstances which prevent the addressee from complying with the request.

Due to the temporary and preliminary nature of the EPsO, the execution of the related EPOC-PR is less restrictive and only requires the addressee to preserve the requested data without undue delay for a period of 60 days, with a possible extension of a further 30 days if necessary to allow for the issuance of a subsequent production order. At the end of this period, the obligation to keep the data shall cease unless the issuing authority confirms the issuing of a subsequent production order. In that case, the addressee shall keep the data for as long as necessary for the production. The obligation to inform the issuing authority of legal or factual circumstances that prevent the addressees from complying with the order also applies to EPOC-PR.

If the addressee doesn't comply with the EPOC or EPOC-PR request, the enforcement procedure can be carried out in accordance with the provisions of Art. 16. During this procedure, the enforcement authority examines the circumstances of the case with regard to the admissibility of the order issued. As a result, the authority may recognise the order and take the necessary measures for its enforcement, or it may decide not to recognise or enforce the order if it concludes that its enforcement is inadmissible. If the enforceability of the EPO has been confirmed by the enforcing authority and the service provider still fails to comply with its request, that authority may impose a fine

of up to 2% of its total worldwide annual turnover in the preceding financial year (Art. 15:1 EPOR).

5. EPOs: Speed of proceedings versus fundamental rights and the rule of law

From the very beginning of the works on the EPOR, both its general idea and certain of its provisions have been the subject of strong criticism due to the potential violation of fundamental standards of criminal procedure, in particular from the point of view of fair trial guarantees in relation to the rights of the suspect. The most common criticism of direct requests for disclosure of electronic evidence has been that, although they are based on the mutual recognition mechanism, they remove a crucial layer of control by the judicial authorities of the enforcing State, unlike traditional cross-border mutual legal assistance mechanisms. The elimination (or at least the limitation) of this principle of bilateral admissibility assessment, which has been repeatedly declared by the European Court of Justice to be one of the cornerstones of international cooperation in criminal cases, may lead to a lack of proper control of production requests from the point of view of their necessity and proportionality to the purpose of the case.[168]

Another serious argument against the EPOs' mechanisms is that they could lead to a general increase in surveillance, which, together with the relatively narrow group of persons protected by immunities, privileges and rules on the limitation of criminal liability that relate to the freedom of the press, could particularly affect independent journalists and political activists, especially in states suffering from deficiencies in the rule of law.[169]

Aware of this threat, the EU legislator has included a number of safeguards in the EPO Regulation. Apart from the aforementioned right of objection of the addressees and the admissibility control carried out by the enforcing authority, the most important safeguards are the so-called information duty and effective remedies.

According to EPOR Art. 13:1, the issuing authority shall without undue delay inform the person whose data are requested of the production of data on the basis of a European Production Order. However, this general rule is weakened by the following paragraph, according to which the issuing authority may delay, restrict or omit to inform the person whose data are requested to the extent and for as long as this constitutes a necessary and proportionate measure in a democratic society, i.e. to avoid obstructing official or legal inquiries, investigations or proceedings or to avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties. As a result, a person whose data has been requested through an EPdO may not even be aware of it until the very last stage of criminal proceeding and, consequently, may be deprived of the possibility to make use of effective remedies to protect his or her rights and freedoms. On the other hand, the person whose data are the subject of the Order may not be a national or even a resident of the EU Member State,

[168] Albus V, 'Fast-Tracking Law Enforcement at the Expense of Fundamental Rights' (*Verfassungsbolg*, 15 June 2023) <https://verfassungsblog.de/fast-tracking-law-enforcement-at-the-expense-of-fundamental-rights>.

[169] Berthélémy C, 'e-Evidence compromise blows a hole in fundamental rights safeguards' (*EDRi*, 7 February 2023) <https://edri.org/our-work/e-evidence-compromise-blows-a-hole-in-fundamental-rights-safeguards>.

which may lead to serious difficulties in informing him or her about the request made and the remedies available. It is also significant that these remedies are not precisely defined in the EPOR, while the Art. 18 provisions are very general and indicative, which may lead to considerable disproportions between the Member States in the field of protection against malpractice in the issuing of EPOs.

There are also some practical considerations that may raise concerns about the functioning of the EPOs, in particular from the point of view of service providers, who will not only have to bear all the costs related to the integration into the decentralised IT system and the processing of requests, but may also be overburdened with an overwhelming number of requests, which may be particularly troublesome for smaller providers. The same argument applies to enforcement authorities, some of which are likely to receive a relatively large number of notifications, further overloading already overburdened judicial systems.[170]

Conclusion

Direct cross-border requests for disclosure of electronic evidence by ICT service providers constitute a significant modifying factor in EU criminal cooperation law, as they represent the first instance of private actors being included within the mutual legal cooperation and recognition system. The possibility of sending the European Production Orders and European Preservation Orders directly to the addressees - service providers - together with the short deadlines for their execution and the fact that the entire procedure can be carried out via the Internet, will lead to a significant reduction in the time needed to obtain electronic evidence, which is particularly valuable due to its volatile nature.

Due to the lack of previous assessments by two judicial authorities, including the important role of the enforcing authority, which examined the order to ensure that it complied with the fundamental principles of criminal procedure, including the rights of the suspect, the EPOs are considered by some researchers to be an instrument of potentially excessive surveillance, providing law enforcement authorities with an unprecedented opportunity to circumvent the procedural safeguards related to the principle of proportionality.

It seems that future practice in the application of these Regulations should address and resolve these doubts, adjust them accordingly and endeavour to minimise the possible risk of violation of fundamental principles of criminal procedure and the rights of its participants. It is worth remembering that the provisions of the discussed regulations will be applicable from 18 August 2026, which gives their addressees sufficient time to consider and identify possible problems and controversies related to their operation, as well as to prepare for their introduction, both in terms of technical issues and with regard to the development of guidelines for good practice. Nonetheless, it is still advisable to wait patiently for the evaluation report on the Regulation, due by 18 August 2029, which will show whether the concerns expressed have been justified.

[170] This applies especially to Ireland, being the seat of the most of European branches of global ICT companies.

CHAPTER III

ENVIRONMENTAL AND SPACE LAW

3.1 The Right to Clean, Healthy and Sustainable Environment in Artificial Intelligence era*

By ***Lucia Bakošová*** (Pavol Jozef Šafárik University)

Introduction

The industrial revolution 4.0 plays a significant role in the development and use of new technologies, such as artificial intelligence (hereinafter "AI"), machine learning, the Internet of Things, or digital twins across industries. These technologies disrupt and change how we produce, do business and live our lives.[171] Especially in the context of sustainable development and climate crisis, the international community turns to new technologies to achieve international commitments stated in the *UN Sustainable Development Goals*[172] or the *Paris Agreement on Climate Change*.[173] In numerous areas, AI enhances the sustainable development and protection of the environment, such as predicting natural disasters, monitoring of deforestation, water degradation, air pollution or farming,[174] as well as improving energy consumption and storage. On the other side, there are also many negative aspects connected to the development and use of AI. Particularly, energy consumption, the need for non-renewable materials (such as lithium, nickel or cobalt) and efficient e-waste management.[175] According to *Vinuesa, Azizpour, Leite et al.* AI can enable the accomplishment of 134 targets across all the *UN Sustainable Development Goals*, but it may also inhibit 59 targets.[176] What still seems to be unclear is the effective regulation of the AI. Due to the special features of the AI, such as inexplicability of its results, potential threat to human rights, accountability etc., special legal regulation that reflects the abovementioned is necessary. Failure to do so could result in gaps in safety, transparency, and ethical standards.[177] As *Volker Türk*, UN High Commissioner for Human Rights highlighted, "regulation of AI and emerging

* The paper presents a partial output within the research project APVV-20-0576 entitled "Green Ambitions for Sustainable Development (European Green Deal in the Context of International and National Law)".

171 See for instance Uygun Y, *Industry 4.0: Principles, Effects and Challenges* (Nova Sci Publ, 2020); Cf. Hamilton Ortiz, J (ed.), *Industry 4.0: Current Status and Future Trends* (IntechOpen, 2020); Kumar K, Zindani D and Davim JP, *Industry 4.0: Developments towards the Fourth Industrial Revolution* (Springer, 2019).

172 UNGA, 'Transforming our world: the 2030 Agenda for Sustainable Development', A/RES/70/1, (2015).

173 Paris Agreement to the United Nations Framework Convention on Climate Change, 12 December 2015, U.N.T.S. Vol. No. 3156.

174 Chui M et al, 'Notes From the AI Frontier: Applying AI for Social Good' (*McKinsey Global Institute*, December 2018) <https://www.mckinsey.com/~/media/mckinsey/featured%20insights/artificial%20intelligence/applying%20artificial%20intelligence%20for%20social%20good/mgi-applying-ai-for-social-good-discussion-paper-dec-2018.ashx>.

175 Leal Filho W et al, 'Deploying Artificial Intelligence for Climate Change Adaptation' (2022) 180 *Technological Forecasting & Social Change* add 121662, p. 2.

176 Vinuesa R, Azizpour H, Leite I et al, 'The role of artificial intelligence in achieving the Sustainable Development Goals' (2020) 11 *Nat Commun* 233.

177 Ibid.

technologies generally needs great care and thoughtfulness. And we must put people at the centre of any solution."[178]

The main focus of the paper is on the interconnection between the emerging international norms on AI and the evolvement of the right to clean, healthy and sustainable environment (hereinafter "R2HE"). The aim of the paper is to answer the question: "Do the adopted or draft international norms regulating the use of AI reflect on the newly recognized right to clean, healthy and sustainable environment? Such aim is fulfilled through analysis of international legally binding, as well as non-binding documents on AI adopted by international organizations, namely the United Nations (hereinafter "UN"), the European Union (hereinafter "EU") and the Council of Europe (hereinafter "CoE"). The author also focuses on the right to clean, healthy and sustainable environment, particularly its content and international recognition. The recognition of this fundamental human right highlights the transformative potential of taking a rights-based approach to the *UN Sustainable Development Goals*.[179]

1. The Right to Clean, Healthy and Sustainable Environment

The international human rights law is, as many branches of public international law are, still developing. In the last years, the focus of the international community is on the recognition of several human rights connected to the environment. The newest addition to the international catalogue of human rights is the R2HE, which was recognized by the UN General Assembly resolution no. 76/300 in July 2022 as a human right.[180] This recognition followed the resolution no. 48/13 of the UN Human Rights Council, which acknowledged the right in October 2021 as a human right that is important for the enjoyment of human rights.[181] Although this right has been recognized, in various forms, in regional agreements[182] and in most national constitutions (there are 110 States where this right enjoys constitutional protection),[183] it has not been adopted in a human rights agreement of global application, and only

[178] OHCHR, TÜRK, V., 'Addressing climate and digital challenges: International Geneva', (2023), <https://www.ohchr.org/en/statements/2023/06/addressing-climate-and-digital-challenges-international-geneva>.

[179] UNGA, Report of the Special Rapporteur on the issue of human rights obligations relating to the enjoyment of a safe, clean, healthy and sustainable environment, David R. Boyd: The human right to a clean, healthy and sustainable environment: a catalyst for accelerated action to achieve the Sustainable Development Goals, A/77/284, (2022), para 22.

[180] UNGA, 'Right to clean, healthy and sustainable environment', A/RES/76/300, (2022), para 1.

[181] UN Human Rights Council, The human right to a clean, healthy and sustainable environment, A/HRC/RES/48/13, (2021), para 1.

[182] See for instance the preamble of the Aarhus Convention (1998); Art. 24 of the African Charter on Human and Peoples' Rights (1991); Art. 38 of the Arab Charter of the Human Rights (2004); Art. 11 of the Protocol of San Salvador (1969).

[183] UN Human Rights Council, Right to a healthy environment: good practices: Report of the Special Rapporteur on the issue of human rights obligations relating to the enjoyment of a safe, clean, healthy and sustainable environment, A/HRC/43/53, 30 December 2019, para 10.

the African Charter on Human and Peoples' Rights, provides for its interpretation in decisions by a review body.[184]

The R2HE, as such, is related to other rights and existing international law,[185] such as the rights to life, the right to enjoy the highest attainable standard of physical and mental health, the right to sufficient food, the right to safe drinking water and sanitation, the right to an adequate standard of living, or the right to development. At the same time, procedural rights, such as the right to participate in decision-making, and access to justice and effective remedies, including the secure exercise of these rights free from reprisals and retaliation are vital to the protection of the environment.[186] Realizing the R2HE also requires international cooperation, solidarity and equity in environmental action, including resource mobilization, as well as recognition of extraterritorial jurisdiction over human rights harms caused by environmental degradation.[187]

Recognition of the R2HE empowers all people with a critical tool to hold their governments, big polluters and all those responsible for environmental harm to account.[188] The R2HE is naturally connected to the concept of sustainable development. Sustainable development according to *Dupuy, Le Moli and Vinuales* may be defined as a development, which as a necessary procedural step, that "takes into account environmental protection (integration), and which does so in a way that is consistent with the environmental treaty obligations undertaken by a country or, at the very least, with the core content of customary international environmental law applicable to all countries."[189] The sustainable development, in its three dimensions (social, economic and environmental), and the protection of the environment, including ecosystems, contribute to and promote human well-being and the full enjoyment of all human rights, for present and future generations.[190] From the historical perspective, first indication of the existence of the R2HE is in the *Stockholm Declaration on the Human Environment (1972)*, which states that "man has the fundamental right to freedom, equality and adequate conditions of life, in an environment of a quality that permits

---

184 UN Human Rights Council, Report of the Special Rapporteur on the Issue of Human Rights Obligations Relating to the Enjoyment of a Safe, Clean, Healthy and Sustainable Environment, A/HRC/37/59, 28 January 2018, para 11.

185 UN Human Rights Council, The human right to a clean, healthy and sustainable environment, A/HRC/RES/48/13, 8 October 2021, para 2.

186 UN Human Rights Council, Report of the Special Rapporteur on the issue of human rights obligations relating to the enjoyment of a safe, clean, healthy and sustainable environment, A/HRC/37/59, 24 January 2018, para 2.

187 UN Human Rights Council, Right to a healthy environment: good practices: Report of the Special Rapporteur on the issue of human rights obligations relating to the enjoyment of a safe, clean, healthy and sustainable environment, A/HRC/43/53, 30 December 2019.

188 UN Human Rights Office of the High Commissioner, UN Environment Programme, UN Development Programme, What is the Right to Healthy Environment? (2023) <https://www.undp.org/sites/g/files/zskgke326/files/2023-01/UNDP-UNEP-UNHCHR-What-is-the-Right-to-a-Healthy-Environment.pdf>.

189 Dupuy PM, Le Moli G and Vinuales JE, 'Customary International Law and the Environment' in Rajamani L and Peel J (eds), *The Oxford Handbook of International Environmental Law*, 2nd edn (OUP, 2021), pp. 385–401.

190 UNGA, 'Right to clean, healthy and sustainable environment', A/RES/76/300, (2022), preamble para 8.

a life of dignity and well-being, and he bears a solemn responsibility to protect and improve the environment for present and future generations."[191]

Another important aspect are the basic obligations of States under human rights law as they relate to the enjoyment of a clean, healthy and sustainable environment. In 2018, the former Special Rapporteur on the Environment, *John H. Knox*, introduced the framework principles on human rights and the environment. The framework principles reflect the application of existing human rights obligations in the environment context. States have obligations under human rights law to protect against environmental harm. The obligations include procedural obligations (such as duties to provide information, facilitate participation and provide access to remedies), substantive obligations (including to regulate private actors) and heightened obligations to those in particularly vulnerable situations.[192] In this chapter, we only highlight those framework principles, which are particularly important in connection to the development and use of AI. In accordance with the framework principles, States should respect, protect and fulfil human rights in order to ensure a safe, clean, healthy and sustainable environment.[193] States should therefore refrain from violating human rights through causing or allowing environmental harm; protect against harmful environmental interference from other sources, including business enterprises, other private actors and natural causes; and take effective steps to ensure the conservation and sustainable use of the ecosystems and biological diversity on which the full enjoyment of human rights depends. States should undertake due diligence to prevent such harm and reduce it to the extent possible, and provide for remedies for any remaining harm.[194] As it was mentioned earlier, the AI has a considerable effect on the environment; therefore, in accordance with Framework principle 8, States should require the prior assessment of the possible environmental impacts of proposed projects and policies, including their potential effect on the enjoyment of human rights.[195] Various stakeholders significantly affect the development and use of AI. Therefore, States should ensure the effective enforcement of their environmental standards against public and private actors,[196] as well as compliance with all applicable environmental and human rights laws. Furthermore, business enterprises should conduct human rights impact assessments in accordance with the *Guiding Principles on Business and Human Rights*.[197] Guiding Principles 18 and 19 provide that businesses should identify and

[191] Declaration of the United Nations Conference on the Human Environment (June 16, 1972). In: *Report of the United Nations Conference on the Human Environment*, UN Doc. A/CONF.48/14/Rev. 1, principle 1.

[192] UN Human Rights Council, Report of the Special Rapporteur on the issue of human rights obligations relating to the enjoyment of a safe, clean, healthy and sustainable environment, A/HRC/37/59, (2018), para 3.

[193] Ibid., Framework principle 2, p. 7.

[194] Ibid., pp. 7–8.

[195] Ibid., p. 11.

[196] UN Human Rights Council, Report of the Special Rapporteur on the issue of human rights obligations relating to the enjoyment of a safe, clean, healthy and sustainable environment, A/HRC/37/59, (2018). Framework principle 12.

[197] UN Office of the High Commissioner for Human Rights, Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework, New York, and Geneva, 2011, <https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf>.

assess any actual or potential adverse human rights impacts with which they may be involved either through their own activities or because of their business relationships. This include meaningful consultation with potentially affected groups and other relevant stakeholders, integrate the findings from their impact assessment across relevant internal functions and processes, and take appropriate action.[198] Lastly, States should cooperate with each other to establish, maintain and enforce effective international legal frameworks in order to prevent, reduce and remedy transboundary and global environmental harm that interferes with the full enjoyment of human rights.[199]

It is important to note, that there is no legally binding document adopted within the UN, EU or the CoE, which would legally recognise the R2HE. There is a proposal for additional protocol to the European Convention on Human Rights and the European Social Charter,[200] however, member States of the CoE in the *Reykjavík Declaration*,[201] which was adopted this year, fell short of delivering a solid commitment to legally recognise this right.

2. Regulation of Artificial Intelligence by International Organizations

The traditional approach of international law to the regulation of emerging technologies has been one of reaction rather than pro-action; only attempting to evaluate and regulate their development or use *ex post facto*. Regulating uncertain, unknown, and even unknowable futures requires flexibility, transparency, accountability, participation by a whole range of actors beyond the State, and the ability to obtain, understand, and translate scientific evidence into law, even while the law remains a force for stability and predictability.[202] Since only a handful of States adopted national regulation of certain aspects of AI,[203] we turn to the role and steps that were taken by selected international organizations, namely the UN, the EU and the CoE, which are particularly active in the preparation of a legally binding legal framework for AI. It is important to note that at the time of writing this paper there is no generally accepted legal definition of AI. The lack of a definition hampers further discussions on possible international cooperation in the analysed area, and in practice, it is difficult to adopt international legislation, the concept and subject of which is not clearly definable.[204] For the purposes of this paper we consider AI as it is defined in the proposal of the EU *Artificial Intelligence Act*,

198 Ibid., Guiding Principle 18 and 19.

199 Ibid., Framework principle 13.

200 Council of Europe – Parliamentary Assembly, Anchoring the right to a healthy environment: need for enhanced action by the Council of Europe, Resolution 2396(2021), 29 September 2021, <https://pace.coe.int/pdf/658d3f594762736ba3c0f378798b2c9529cf4be34aa45a8c38616ecd18fa80c0/res.%202396.pdf>.

201 Council of Europe, 'United Around Our Values' (Reykjavík Declaration), 16 – 17 May 2023, <https://edoc.coe.int/en/the-council-of-europe-in-brief/11619-united-around-our-values-reykjavik-declaration.html>.

202 Brownsword R, Scotford E, Yeung K (eds), *The Oxford Handbook of Law, Regulation and Technology* (OUP, 2017), pp. 500–501.

203 See The OECD Artificial Intelligence Policy Observatory <https://oecd.ai/en/policy-areas>.

204 Klučka J, 'General Overview of the Artificial Intelligence and International Law' in Klučka J, Bakošová L, and Sisák Ľ (eds), *Artificial Intelligence from the Perspective of Law and Ethics: Contemporary Issues, Perspectives and Challenges* (Nakladatelství Leges, 2021), p. 13.

which is defined as a "software that is developed with one or more of the techniques and approaches listed in Annex I[205] and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with.[206] Furthermore, at the time of writing this paper, there is no international legal framework on AI, although some legal aspects of the development and use of AI[207] are regulated by soft-law instruments, such as codes of conduct or recommendations.[208]

2.1 The United Nations Regulation on AI in the Context of the Right to Clean, Healthy and Sustainable Environment

The UN, as a universal international organization provides appropriate forum for establishing a common approach to the adoption of legal standards on AI. In the past several years, numerous documents and reports were published concerning the future regulation of AI, for instance *The Age of Digital Interdependence (2019),*[209] *A United Nations system-wide strategic approach and road map for supporting capacity development on artificial intelligence (2019),*[210] *the UN Secretary General's Roadmap for Digital Cooperation (2020),*[211] *the UN Secretary-General's Our Common Agenda report (2021)*,[212] or the *Principles for the Ethical Use of AI in the UN System (2022)* (hereinafter "Principles").[213] So far, the mentioned documents, apart from the *Principles for the*

[205] (a) Machine learning approaches, including supervised, unsupervised and reinforcement learning, using a wide variety of methods including deep learning; (b) Logic- and knowledge-based approaches, including knowledge representation, inductive (logic) programming, knowledge bases, inference and deductive engines, (symbolic) reasoning and expert systems; (c) Statistical approaches, Bayesian estimation, search and optimization methods.

[206] European Commission, Proposal for a Regulation of the European Parliament and of the Council on Artificial Intelligence (Artificial Intelligence Act), Brussels, 21 April 2021, 2021/0106(COD), Art. 3.

[207] See for instance in Klučka J, Bakošová L, and Sisák Ľ (eds), *Artificial Intelligence from the Perspective of Law and Ethics: Contemporary Issues, Perspectives and Challenges* (Nakladatelství Leges, 2021); Rayfuse R, 'Public International Law and the Regulation of Emerging Technologies' in Brownsword R, Scotford E, and Yeung K (eds), *The Oxford Handbook of Law, Regulation and Technology* (OUP, 2017); DiMatteo LA, Poncibò C, and Cannarsa M (eds), *The Cambridge Handbook of Artificial Intelligence: Global Perspectives on Law and Ethics* (CUP, 2022).

[208] See for instance OECD, 'Principles on Artificial Intelligence', OECD/LEGAL/0449, (2019) <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449>; Global Partnership on AI Report, 'Climate Change AI and Centre for AI & Climate, Climate Change and AI: Recommendations for Government' (*GPAI*, November 2021) <https://www.gpai.ai/projects/climate-change-and-ai.pdf>.

[209] Anchoring the right to a healthy environment UN Secretary-General's High-level Panel on Digital Cooperation, The Age of Digital Interdependence, (2019), <https://www.un.org/en/pdfs/DigitalCooperation-reportfor%20web.pdf>.

[210] UN, A United Nations system-wide strategic approach and road map for supporting capacity development on artificial intelligence, (2019), CEB/2019/1/Add.3, <https://unsceb.org/sites/default/files/2020-09/CEB_2019_1_Add-3-EN_0.pdf>.

[211] UNGA, 'Roadmap for digital cooperation: implementation of the recommendations of the High-level Panel on Digital Cooperation: Report of the Secretary General', A/74/821, (2020).

[212] UN, Our Common Agenda: Report of the Secretary-General, United Nations, New York, (2021) <https://www.un.org/en/content/common-agenda-report/assets/pdf/Common_Agenda_Report_English.pdf>.

[213] United Nations Inter-Agency Working Group on Artificial Intelligence, Principles for the Ethical Use of Artificial Intelligence in the United Nations System, (2022) <https://unsceb.org/sites/default/

Ethical Use of Ai in the UN System, only outlined the future steps that are necessary in order to draft and adopt legally binding framework on AI and three foundational pillars, namely peace and security, human rights and development.[214] The Principles, although are of a non-binding nature, they reflect the core ethical principles that are present in most ethical codes on AI. The aim of the Principles is to provide a basis for UN system organizations to make decisions about how to develop, design, deploy and use AI systems, including multiple interacting AI systems, in a way that is trustworthy and puts human dignity, equality of all human beings, preservation of the environment, biodiversity and ecosystems, respect for cultural diversity, and data responsibility at the centre.[215] Particularly relevant principles in the context of the R2HE, are: (a) do no harm; (b) safety and security; (c) sustainability; (d) responsibility and accountability.

In October 2023, the UN Secretary-General has convened a multi-stakeholder High-level Advisory Body on AI to undertake analysis and advance recommendations for the international governance of AI, in accordance with the *Roadmap for Digital Cooperation*. The advisory body comprises UN member states, relevant UN entities, interested companies, academic institutions and civil society groups.[216] The Body will offer diverse perspectives and options on how AI can be governed for the common good, aligning internationally interoperable governance with human rights and the *UN Sustainable Development Goals*.[217]

The future regulation of the AI within the UN is not only associated with the newly established advisory body, but also with the adoption of the *Global Digital Compact*, which is to be adopted during a Summit of the Future, which is to be held on 22 and 23 September 2024, in New York. In May 2023, the UN Secretary-General issued a policy brief for the *Global Digital Compact*, outlining areas in which 'the need for multistakeholder digital cooperation is urgent', and among them was the governance AI for humanity. Among the objectives and actions to advance such cooperation is putting human rights at the centre of the digital future. One key proposed action is the establishment of a digital human rights advisory mechanism, facilitated by the Office of the UN High Commissioner for Human Rights, to provide guidance on human rights and technology issues. The brief also addresses agile governance of AI and other emerging technologies. The proposed objectives relate to ensuring transparency, reliability, safety, and human control in the design and use of AI; putting transparency,

---

files/2022-09/Principles%20for%20the%20Ethical%20Use%20of%20AI%20in%20the%20UN%20System_1.pdf>.

[214] Anchoring the right to a healthy environment UN Secretary-General's High-level Panel on Digital Cooperation, The Age of Digital Interdependence, (2019), <https://www.un.org/en/pdfs/DigitalCooperation-reportfor%20web.pdf>.

[215] United Nations Inter-Agency Working Group on Artificial Intelligence, Principles for the Ethical Use of Artificial Intelligence in the United Nations System, 20 September 2022, pp. 2–3.

[216] UN, A United Nations system-wide strategic approach and road map for supporting capacity development on artificial intelligence, (2019), CEB/2019/1/Add.3, <https://unsceb.org/sites/default/files/2020-09/CEB_2019_1_Add-3-EN_0.pdf>, para 88.

[217] UN, UN Secretary-General launches AI Advisory Body on risks, opportunities, and international governance of artificial intelligence, Press release, (2023), <https://www.un.org/sites/un2.un.org/files/231025_press-release-aiab.pdf>.

fairness, and accountability at the core of AI governance; and combining existing norms, regulations, and standards into a framework for agile governance of AI.[218] Since there is no draft version of the Compact at the time of writing of this paper, it is questionable whether it will require States and other actors to respect, protect and fulfil the R2HE as a specifically mentioned human right. However, as it is common for UN documents on AI, only a vague reference to human rights is present in the documents. Furthermore, even if the *Global Digital Compact* is adopted, as such it will not be an international treaty, but only a non-binding document.

2.2 The European Union's AI Act

Probably the most active international organization on the issue of AI is the EU. The EU's ambition is to be the leading actor in AI, aiming to boost research, industrial capacity and ensure protection of human rights and fundamental freedoms. Since 2018, the EU adopted several documents on AI,[219] however, in this paper we only focus on the draft of *Artificial Intelligence Act*[220] (hereinafter "AI Act") and its regulation in the context of the R2HE. The extraterritorial application of the *AI Act* and its likely demonstration effect for policymakers means that the *AI Act* will have a range of implications for the development of AI regulation globally, as well as efforts to build international cooperation on AI.[221] The *AI Act* focuses exclusively on the high-risk AI systems, which are defined as those that are part of a product falling under the EU product safety regulation or belong to a list of stand-alone high-risk AI systems laid down by the proposal, such as AI systems assessing the creditworthiness of individuals or used in the context of recruitment.[222] When it comes to the requirements for High-risk AI systems, Art. 9 states that a risk management system shall be established, implemented, documented and maintained in relation to high-risk AI systems and it shall consist of a continuous

---

[218] UN, Our Common Agenda Policy Brief 5: A Global Digital Compact – an Open, Free and Secure Digital Future for All, (2023) <https://indonesia.un.org/sites/default/files/2023-07/our-common-agenda-policy-brief-gobal-digi-compact-en.pdf>, p. 10.

[219] See for instance: European Commission: Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions: Artificial Intelligence for Europe, 25 April 2018, COM/2018/237; European Commission: Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – Fostering a European Approach to Artificial Intelligence, Brussels, 21 April 2021, COM(2021) 205 final; European Commission: Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions: Coordinated Plan on Artificial Intelligence, 7 December 2018, COM(2018) 795; European Commission: White Paper on Artificial Intelligence – A European approach to excellence and trust, Brussels, 19 February 2020, COM(2020) 65 final.

[220] European Commission, Proposal for a Regulation of the European Parliament and of the Council on Artificial Intelligence (Artificial Intelligence Act), Brussels, 21 April 2021, 2021/0106(COD).

[221] Meltzer J, Tielemans A, 'The European Union AI Act: Next steps and issues for building international cooperation' (*Global Economy and Development at Brookings*, 1 June 2022) <https://www.brookings.edu/articles/the-european-union-ai-act-next-steps-and-issues-for-building-international-cooperation-in-ai/>.

[222] European Commission, Proposal for a Regulation of the European Parliament and of the Council on Artificial Intelligence (Artificial Intelligence Act), Brussels, 21 April 2021, 2021/0106(COD), Art. 6.

iterative process run throughout the entire lifecycle of a high-risk AI system, requiring regular systematic updating.[223]

The proposal for the *AI Act* does not refer to R2HE, but to the right to a high level of environmental protection and the improvement of the quality of the environment including in relation to the health and safety of people. The obligations for *ex ante* testing, risk management and human oversight will also facilitate the respect of other fundamental rights by minimising the risk of erroneous or biased AI-assisted decisions in critical areas such as education and training, employment, important services, law enforcement and the judiciary.[224]

Solís Peréz, the Rapporteur of the Committee on the Environment, Public Health and Food Safety of the European Parliament in opinion from 22 April 2022 is concerned that the *AI Act* does not provide sufficient protection to the environment and by implication the protection of the R2HE.[225] Therefore, the Rapporteur proposed that the *AI Act* shall include the environment among the areas that require a high level of protection. In order to do so, the environment has been included in all the recitals and articles together with health, safety and the protection of fundamental rights. This will entail the classification as "high risk AI" of all those systems that can have major negative implications on the environment. At the same time, the Rapporteur has reinforced the right to proper redress mechanisms in case of negative environmental impacts as set out in the Aarhus Convention and has set the principle of "Do no significant harm" as established in the Taxonomy Regulation as a limit to ensure that AI systems abide with the EU's high level of environmental standards and rights.[226]

The European Parliament and the Council, subsequently, made amendments to the Commission's proposal and included provisions that reflect the R2HE, but not expressly stating the right. For instance, under art. 1, the purpose of this Regulation is to promote the uptake of human-centric and trustworthy AI and to ensure a high level of protection of health, safety, fundamental rights, democracy and rule of law and the environment from harmful effects of AI systems in the Union while supporting innovation.[227] Under

---

[223] Ibid., Art. 9 (1) and (2).

[224] Ibid., p. 11.

[225] European Parliament – Committee on the Environment, Public Health and Food Safety, Opinion of the Committee on the Environment, Public Health and Food Safety for the Committee on the Internal Market and Consumer Protection and for the Committee on Civil Liberties, Justice and Home Affairs on the proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts COM(2021)0206 – C9-0146/2021 – 2021/0106(COD), 22 April 2022, <https://artificialintelligenceact.eu/wp-content/uploads/2022/05/AIA-ENVI-Rule-56-Opinion-Adopted-22-April.pdf>, p. 3.

[226] Ibid., pp. 3–4.

[227] European Parliament, Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts COM(2021)0206 – C9-0146/2021 – 2021/0106(COD), <https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_EN.pdf>, amendment 140. See also Council of the European Union, Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts - General approach, Brussels, 25 November 2022, 14954/22 <https://data.consilium.europa.eu/doc/document/ST-14954-2022-INIT/en/pdf>.

general principles applicable to all AI systems (art. 4 a letter (f)), AI systems shall be developed and used in a sustainable and environmentally friendly manner as well as in a way to benefit all human beings, while monitoring and assessing the long-term impacts on the individual, society and democracy.[228]

2.3 The Council of Europe

The Committee of Ministers of the CoE has tasked the Committee on Artificial Intelligence with elaborating a legally binding instrument on the development, design and application of AI systems based on the CoE's standards on human rights, democracy and the rule of law. In July 2023, the consolidated working draft of the Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law (hereinafter "Convention") was made public. The purpose and object of the Convention is to set out principles and obligations aimed at ensuring that design, development, use and decommissioning of AI systems are fully consistent with respect for human dignity and individual autonomy, human rights and fundamental freedoms, the functioning of democracy and the observance of the rule of law.[229] The Convention shall apply to design, development, use and decommissioning of AI systems that have the potential to interfere with the respect for human rights and fundamental freedoms, the functioning of democracy and the observance of rule of law, but shall not apply to research and development activities regarding AI systems unless the systems are tested or otherwise used in ways that have the potential to interfere with human rights and fundamental freedoms, democracy and the rule of law.[230] The scope of the Convention formulated in this way provides a wide scope for interpretation as to whether a certain AI system falls under the Convention or not. In our opinion, a more precise definition of scope is necessary.

The Convention is built on the principles of (a) transparency and oversight; (b) accountability and responsibility; (c) equality and non-discrimination; (d) privacy and personal data protection; (e) safety, security and robustness; (f) safe innovation.[231] All of the mentioned principles are present in most codes of ethics on AI.[232] In order to give full effect to the principles and obligations set out in this Convention, each Party shall maintain and take such graduated and differentiated measures in its domestic legal system as may be necessary and appropriate in view of the severity and probability of

---

[228] Ibid, Amendment 213.

[229] Council of Europe – Committee on Artificial Intelligence, Consolidated working draft of the Framework Convention on Artificial Intelligence, Hu-man Rights, Democracy and the Rule of Law, 7 July 2023, CAI(2023)18, <https://rm.coe.int/cai-2023-18-consolidated-working-draft-framework-convention/1680abde66>, Art. 1.

[230] Ibid., Art. 4, para 1 and 2.

[231] Ibid., Art. 7–12.

[232] See for instance United Nations Inter-Agency Working Group on Artificial Intelligence, Principles for the Ethical Use of Artificial Intelligence in the United Nations System, (2022) <https://unsceb.org/sites/default/files/2022-09/Principles%20for%20the%20Ethical%20Use%20of%20AI%20in%20the%20UN%20System_1.pdf>; Floridi L, Cowls J, Beltrametti M et al, 'AI4People — An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations' (2018) 28 *Minds and Machines* 689.

occurrence of adverse impacts on human rights and fundamental freedoms, democracy and the rule of law during design, development, use and decommissioning of AI systems.[233] In accordance with art. 5 of the draft Framework Convention, each Party shall take the necessary measures to ensure that all activities in relation to the design, development, use and decommissioning of AI systems are compatible with relevant human rights and non-discrimination obligations undertaken by it under international law, or prescribed by its domestic law.[234] However, there is no mention of the R2HE, or the sustainable development or the protection of the environment in the proposal of the Convention. Since the formulation of the art. 5 is a bit vague, we argue that the R2HE, since it is a human right important for the enjoyment of other (fundamental) human rights and most CoE Member States provide constitutional protection to the R2HE, Parties to the proposed Convention will be obliged to take necessary steps to respect, protect and fulfil the R2HE.

On the positive side, the proposed Convention contains risk and impact management framework (art. 15), under which States shall take measures for the identification, assessment, prevention and mitigation of risks and impacts to human rights, democracy and rule of law arising from the design, development, use and decommissioning of AI. Such measures shall (a) contain adequate requirements which take due account of the context and intended use of AI, in particular as concerns risks to human rights, democracy, the rule of law and the preservation of the environment; (b) take account of the severity, duration and reversibility of any potential risks and adverse impacts; and (c) ensure that the risk and impact management processes are carried out iteratively throughout the design, development, use and decommissioning of the AI.[235] What is particularly worth mentioning is the art. 26, under which Parties that are members of the EU shall, in their mutual relations, apply EU rules governing the matters within the scope of this Convention. Although, the *AI Act* does not contain the R2HE, several proposed provisions require EU member States to protect the environment from harmful effects of AI.

Conclusion

This brings us back to the main question: **"Do the adopted or draft international norms regulating the use of AI reflect on the newly recognized right to clean, healthy and sustainable environment?"** First, it is important to note that are still no international legal frameworks regulating the development and use of AI. All of the analysed documents were of non-binding nature, either due to the fact that these are only recommendations or that they are currently only draft legal frameworks. It seems that the proposed regulation of the EU will be the first legally binding instrument in this area.

Second, the R2HE is not expressly recognized in legally binding instruments of the UN, EU or the CoE. Although, the Parliamentary Assembly of the CoE

[233] Council of Europe – Committee on Artificial Intelligence, Consolidated working draft of the Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law, 7 July 2023, CAI(2023)18, Art. 2.

[234] Ibid., Art. 5.

[235] Ibid., Art. 15.

recommended the adoption of an additional protocol to the European Convention on Human Rights and the European Social Charter, member States are still hesitant to make another commitment and to open themselves to potential lawsuits. Adoption of such an instrument would give the European Court of Human Rights a base for rulings concerning human rights violations arising from environment-related adverse impacts on human health, dignity and life. Victims would have an easier way to lodge applications for remedies and would also act as a preventive mechanism to supplement the currently rather reactive case law of the European Court of Human Rights.

Third, the analysed proposed legal frameworks on AI no do not specifically require States and relevant stakeholders to respect, protect and fulfil the R2HE as such. However, States and actors are required to protect "the relevant human rights." We argue, that the R2HE is very much a relevant human right that the development and use of AI may violate, especially due to the fact, that the R2HE is connected to the enjoyment of fundamental human rights. Currently, it seems, that the protection of the R2HE in the context of development and use of AI is mainly ensured by domestic courts, through constitutional protection, rather than the international law or international regulation on AI.

3.2 International Legal Mechanisms of the Protection of Biological Diversity in the Context of Current Technologies*

By ***Juraj Panigaj*** (Pavol Jozef Šafárik University)

Introduction

> *"Technology is a gift of God. After the gift of life, it is perhaps the greatest of God's gifts. It is the mother of civilizations, of arts and sciences."*[236]

It is fair to say international law, or law in general, is quite complex. But it is not a match for the complexity of nature, its ecosystems, and all its living and non-living parts. Biodiversity is an integral part of nature, and it means, in accordance with Convention on Biological Diversity, *"the variability among living organisms from all sources including, inter alia, terrestrial, marine and other aquatic ecosystems and the ecological complexes of which they are part; this includes diversity within species, between species and of ecosystems."*[237] Within this article, we try to analyze the relationship between biodiversity and technology, primarily from the legal perspective. Of course, before we analyze certain international treaties, we consider it important to pay an attention to the issue in question in a more general manner. That being said, we start the paper with some "calculations," that should highlight the severity of the situation, and necessity for proper regulation, but mostly application of set rules. Later, as already mentioned, the paper discusses technology-biodiversity relationship from the perspective of certain international environmental treaties. In regard to biodiversity the article deals in the beginning only with the biodiversity of animal species.

1. Biodiversity and technology in numbers

As the quote of Freeman Dyson from the beginning implies, above the technology there is the "*gift of life."* This is all connected with the issue of biodiversity because it is one of the cornerstones, necessary for all life on Earth, including humans.[238] It seems humanity is quite aware of the importance of biodiversity, but awareness is only a first step. A quick look at the numbers shows us, that as humanity, we did not take many steps so far.

In the last 50 years, wildlife populations have shrunk by 69% on average.[239] In the South America region, where the Amazon Forest lies, decline is the most severe,

* This article was processed with the support of the project APVV-20-0576 under the title "Green ambitions for sustainable development (European Green Deal in the Context of International and Domestic law".

[236] Brynjolfsson E, McAfee A, *The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies* (Norton, 2014), p. 6.

[237] Convention on Biological Diversity, June 5, 1982, reprinted in 31 ILM 822 (1992), Art. 2.

[238] 'Why is biodiversity important?' (*The Royal Society*) <https://royalsociety.org/topics-policy/projects/biodiversity/why-is-biodiversity-important/> accessed 1 November 2023.

[239] Greenfield P, 'The biodiversity crisis in numbers – a visual guide' (*The Guardian*, 1 December 2022) <https://www.theguardian.com/environment/2022/dec/06/the-biodiversity-crisis-in-numbers-a-visual-guide-aoe> accessed 1 November 2023.

and numbers are above 90%.[240] In comparison, a decline in Europe and Central Asia is somewhere around 18%. Such a plunge does not mean 70% of life disappeared. It means "only" populations (biomass itself) have shrunk.[241] Another study has also shown alarming results. So far, we believed, only 28% of life on earth is threatened with extinction. However, the study shows these numbers go up to 48%,[242] and only 3% of species show signals of recovery.[243] Except for the latter, all the above numbers keep rising. The indicated numbers demand a quick response. On the other hand, we need to point out that "only" 1.7 million species have been discovered so far.[244] Some sources report higher numbers up to 2.13 million, but there is an assumption that 20% of it is made of duplicates and synonyms.[245] But we still do not know how many species are on earth in total, and even the assumptions are a wild guess, something between 3 million to 100 million species (some scientists claim it could be even 1 trillion species[246]).[247]

To connect the above with technology, we would like to quote Tanya Steele, chief executive at World Wide Fund for Nature UK, who said: *"The climate and nature crises, their fates entwined, are not some faraway threat our grandchildren will solve with still-to-be-discovered technology."*[248] That being said, it is the technology of "today" which should save tomorrow. But what are the numbers behind technology?

We are not able to assume the number of investments regarding the specific technology concerning biodiversity itself. Only a more general assumption is possible. In general, investments in "green tech" are increasing annually. In 2021 it was globally approximately 755 billion U.S. dollars (still only one-third of what is necessary to eliminate net carbon emissions by 2050).[249] In comparison, in the USA itself, investments in IT crossed the one trillion U.S. dollar mark.[250] For example, so-called

---

240 Ibid.

241 Ibid.

242 Finn C, 'Global loss of biodiversity is significantly more alarming than previously suspected' (*Queen's University Belfast*, 23 May 2023) <https://www.qub.ac.uk/News/Allnews/2023/Globallossofbiodiversityissignificantlymorealarmingthanpreviouslysuspected.html> accessed 1 November 2023.

243 Ibid.

244 Tangley L, 'How Many Species Exists' (*The National Wildlife Federation*, 1 December 1998) <https://www.nwf.org/Magazines/National-Wildlife/1999/How-Many-Species-Exist> accessed 2 November 2023.

245 Almost half of all the species consist of insects.

246 Lennon JT, Locey KJ, 'Earth may be home to one trillion species' (*ScienceDaily*, 2 May 2016) <https://www.sciencedaily.com/releases/2016/05/160502161058.htm> accessed 2 November 2023.

247 Ritchie H, 'How many species are there?' (*Our World in Data*, 30 November 2022) <https://ourworldindata.org/how-many-species-are-there> accessed 2 November 2023.

248 Greenfield P, Benato M, 'Animal populations experience average decline of almost 70% since 1970, report reveals' (*The Guardian*, 13 October 2021) <https://www.theguardian.com/environment/2022/oct/13/almost-70-of-animal-populations-wiped-out-since-1970-report-reveals-aoe> accessed 2 November 2023.

249 Relander B, 'Investing in Green Technology' (*Investopedia*, 31 July 2022 <https://www.investopedia.com/articles/investing/040915/investing-green-technologythe-future-now.asp> accessed 2 November 2023.

250 'Information technology (IT) investments worldwide in 2021, by country' (*Statista*) <https://www.statista.com/statistics/1331124/global-it-investments-by-country/> accessed 1 November 2023.

"climate tech" nowadays includes multibillion wide-ranging businesses across multiple fields, and some authors predict a bright future for this area of technology.[251]

2. Current relationship between technology and biodiversity

This chapter will be divided into 2 parts. The first one will deal with technology in more of a literal form, while the second one will deal with biotechnology.

2.1 Technology versus biodiversity

Talking about technology, its "bio-form" is not the first example in our minds. Computers, artificial intelligence, drones, etc. are the ones, that pop up in our heads first. And those are also the technologies we will briefly analyze below.

Technology holds enormous potential in relation to the protection of biodiversity. On the other hand, its use should be a last resort.[252] Without further delay, what are currently the best adepts for biodiversity protection?

Several studies have been conducted focused on current technologies and their potential to slow biodiversity loss down. One particular study showed, that among other technologies, machine learning and computer vision, eDNA[253] and genomics, and networked sensors (camera traps, biosensors, tracking devices, etc.[254]) seem to have the highest potential. Secondly, conservationists opine that the biggest challenges standing in the way of technology are mostly finance-related issues and inadequate capacity-building.[255] And these are just problems related to the application itself.

For example, drones have potential, which has been already demonstrated. Nowadays they are easily accessible. But if we want them to properly monitor animals, people, or even detect poachers, we need drones with military-level capabilities. However, drones with these specifications are currently too expensive.[256] Also, we can't forget another issue with technologies like drones, camera traps, and other "surveillance" technologies, namely privacy concerns.

Technology is expensive. It is a simple fact, but it hampers the use of technology to its full potential. The severity of this issue can be demonstrated as follows. The

---

[251] Sonnenfeldt M, 'It took 30 years for climate tech investments to pay off. Now they're best placed to survive the VC winter' (*FORTUNE*, 26 July 2023) <https://fortune.com/2023/07/26/climate-tech-investments-pay-off-best-placed-survive-vc-winter-venture-capital-tech-environment/> accessed 1 November 2023.

[252] Conway W, 'Chapter 30: Can Technology Aid Species Preservation?' in Wilson EO and Peter FM (eds), *Biodiversity* (NAS/SI, 1999), pp. 263–268.

[253] eDNA, or so-called environmental DNA, is DNA collected from a variety of environmental samples (soil, snow etc.), rather than sampled from individual organism.

[254] Davis E, 'First-ever State of Conservation Technology' Report Identifies Top 3 Emerging Technologies to Advance Conservation' (WWF, 15 December 2021) <https://www.worldwildlife.org/press-releases/first-ever-state-of-conservation-technology-report-identifies-top-3-emerging-technologies-to-advance-conservation> accessed 1 November 2023.

[255] Speaker T, O'Donnell S, Wittemyer G et al, 'A Global Community-Sourced Assessment of the State of Conservation Technology' (2022) 36(3) *Conserv Biol* 13871.

[256] Pimm SL, Alibhai S, Bergl R et al, 'Emerging Technologies to Conserve Biodiversity' (2015) 30(11) *Trends Ecol Evol* 685.

main cause of the extinction of wildlife is natural habitat loss.[257] At the same time, the capability and the necessary finances are located in developed countries, while the most diverse and yet the most threatened habitats are located in poor developing countries.[258] Without the help of developed countries, it is impossible for developing countries to successfully fight biodiversity loss. As it will be shown later, international environmental law has been trying to regulate this specific problem.

We already mentioned so-called networked sensors. Camera traps, tracking devices, or other monitoring devices have been used for decades, but even though they have come a long way, they still can pose a danger to animals, especially endangered ones. As with drones, these devices are quite expensive. To use a tracking device, you need to physically capture animals, and for endangered species, even the least intrusive device may pose a threat.[259] Bioacoustics are another interesting type of networked sensors. A recent study showed their potential for monitoring the success of biodiversity recovery. Since many species, including birds, mammals, amphibians, and insects use sound to communicate, using bioacoustics helps monitor biodiversity development, and even potentially discover new species.[260] After these technologies "finish their jobs", artificial intelligence analyzes gathered information. AI has the potential to identify and detect important information out of thousands of photos or out of hours of field recording – reducing the time and costs of manual labor.[261]

Technologies have the potential to be a reliable partner in the field of biodiversity protection. Later, we will analyze whether this area is adequately regulated by international environmental law. Does environmental law regulate the use of the abovementioned technologies, does it address challenges such as limited funding, inadequate capacity-building, data sharing, or privacy concerns?

2.2 Biotechnology versus biodiversity

When it comes to biotechnology, it is already a well-established type of technology in international environmental law. However, before we look at it from a legal perspective, it is necessary to point out its pros and cons.

In accordance with the Convention on Biological Diversity (1992), *"biotechnology means any technological application that uses biological systems, living organisms, or derivatives thereof, to make or modify products or processes for specific use."*[262] Examples

---

[257] Lebleu T, 'Technologies to protect biodiversity' (*Solarimpulse Foundation*, 18 April 2019) <https://solarimpulse.com/news/technologies-to-protect-biodiversity#> accessed 2 November 2023.

[258] Conway W, 'Chapter 30: Can Technology Aid Species Preservation?' in Wilson EO and Peter FM (eds), *Biodiversity* (NAS/SI, 1999), pp. 263–268.

[259] Pimm SL, Alibhai S, Bergl R et al, 'Emerging Technologies to Conserve Biodiversity' (2015) 30(11) *Trends Ecol Evol* 685.

[260] Müller J, Mitesser O, Schaefer HM et al, 'Soundscapes and Deep Learning Enable Tracking Biodiversity Recovery in Tropical Forests' (2023) 14 *Nat Commun* 6191.

[261] Speaker T, O'Donnell S, Wittemyer G et al, 'A Global Community-Sourced Assessment of the State of Conservation Technology' (2022) 36(3) *Conserv Biol* 13871.

[262] Convention on Biological Diversity, June 5, 1982, reprinted in 31 ILM 822 (1992).

of biotechnology include cloning, genome editing, cryopreservation, artificial insemination, etc.[263]

Biotechnology already presents a useful tool for biodiversity protection; however, its true potential remains yet to be discovered. Biotechnology should be able to suppress invasive alien species and increase the immunity of species or their resilience to environmental threats.[264] Another positive side of biotechnology lies for example in storing genetic material, so-called cryopreservation. On the other hand, there is something true behind the 30-year-old statement: "*Sustaining species in a freezer, in a captive population, or small, fragmented refuges provides little to the Earth in the way of basic ecological services.*"[265]

Where are pluses, there are minuses. In relation to biotechnology, we can say there are even threats regarding its application. The use of biotechnology to boost biodiversity might eventually threaten biodiversity itself.

Some of the risks of using genetically modified organisms may consist of the following. An organism may develop an increased ability to establish and spread in an environment, potentially competing with native species, and reducing natural biodiversity.[266] There are also concerns in the scientific community that, for example, the use of biotechnologically derived seeds could lead to the loss of genetic diversity between individual crops, as native species would be replaced in the same way that modern "hybrids" have replaced many traditional varieties or breeds. There could also be an uncontrollable transfer of certain structures, e.g., those that determine resistance to pesticides, pests, or plant diseases, and as a result of that so-called superweeds might be created that would be capable of displacing other local fauna, thereby reducing biodiversity as such.[267]

Biotechnology carries bigger threats than other types of technology. That's why it needs to be properly regulated not only by domestic legislation but also by international environmental law. That is also the reason, why international law pays more attention to this type of technology than others.

3. Technologies and international environmental law

Regulation of technology in relation to biodiversity, by tools of international environmental law, is a quite narrow and specific issue. We will now analyze currently the most relevant international environmental treaties, such as the Convention on

---

263 Guerrero S, 'How biotech aids biodiversity' (*Alliance for science*, 17 February 2022) <https://allianceforscience.org/blog/2022/02/how-biotech-aids-biodiversity/> accessed 1 November 2023.

264 Macfarlane NBW et al, 'Direct and Indirect Impacts of Synthetic Biology on Biodiversity Conservation' (20 October 2022) 25(11) *iScience* 105423.

265 Conway W, 'Chapter 30: Can Technology Aid Species Preservation?' in Wilson EO and Peter FM (eds), *Biodiversity* (NAS/SI, 1999), pp. 263–268.

266 'Environmental Risk Assessment of the Products of Biotechnology' (*Australian Government, Department of Agriculture, Water and the Environment*) <https://www.awe.gov.au/environment/protection/biotechnology> accessed 1 November 2023.

267 Nezhmetdinova FT et al, 'Risks of Modern Biotechnologies and Legal Aspects of Their Implementation in Agriculture' (2020) 17 *BIO Web of Conferences* 227.

Biological Diversity and its protocol, the Cartagena Protocol on Biosafety, and the Agreement under the United Nations Convention on the Law of the Sea on the conservation and sustainable use of marine biological diversity of areas beyond national jurisdiction (hereinafter also as "*The High Sea Treaty*").

3.1 Convention on Biological Diversity

When it comes to biodiversity protection, the primary treaty of concern should be the Convention on Biological Diversity (hereinafter referred to as "*CBD*" or "*Convention*"). CBD is the cornerstone of the protection of biodiversity by international environmental law. It is mostly because of its framework character, and of course, because it has over 190 contractual parties. Only after the adoption of CBD was the protection of biodiversity specifically targeted.[268] Since CBD is a framework convention, it does not establish standards for the protection of biodiversity, yet it offers foundations for biodiversity protection mainly in the form of *in situ* conservation, but also for restoration of deteriorated ecosystems and gene bank management.[269] Technologies are an integral part of one of the main objectives of CBD.[270]

On the one hand, CBD defines both biotechnology and technology, but on the other one, it does not. To explain the previous sentence, we need to look at both "definitions." Biotechnology means *"any technological application that uses biological systems, living organisms, or derivatives thereof, to make or modify products or processes for specific use."*[271] Regarding technology itself, CBD states that *"technology includes biotechnology."*[272]

The main difference between these definitions is that the "technology one" does not provide any interpretation of what should be considered technology, only that it includes biotechnology. Since it does not specify, what the technology means (besides biotechnology) for the CBD, it allows us to interpret it far too broadly. The lack of proper definition has the potential to be interpreted incorrectly. To find an example, we do not have to travel far away. For example, there is an official Slovak translation of the CBD in the Notification by the Ministry of Foreign Affairs of the Slovak Republic no. 34/1996 Coll. In the Slovak version, the definition of technology is interpreted completely differently: *"Technology means biotechnology,"* or in Slovak: *"Technológia znamená biotechnológiu."*[273] As we can see, it completely changes the meaning of the word "technology." But there is still a possibility it was just an incorrect translation, not caused by lack of definition.

However, from the context of the other provisions of the Convention, definition of technology does not cover only biotechnology. IUCN Environmental Law Centre

---

[268] Dupuy PM and Vinuales JE, *International Environmental Law: Second Edition* (CUP, 2018), p. 234.

[269] Louka E, *International Environmental Law: Fairness, Effectiveness and World Order* (CUP, 2006), p. 300.

[270] "[…] including by appropriate access to genetic resources and by appropriate transfer of relevant technologies, taking into account all rights over those resources and to technologies, and by appropriate funding." Convention on Biological Diversity, June 5, 1982, reprinted in 31 ILM 822 (1992).

[271] Ibid.

[272] Ibid.

[273] *Notification by the Ministry of Foreign Affairs of the Slovak Republic No. 34/1996 Coll.* (1996).

issued "*A Guide to the Convention on Biological Diversity*" (1994), where we can find the proof for the previous sentence. It can be found in paragraph 1[274] of Article 16 of CBD, and the commentary to this paragraph, which states: *"Developed countries were particularly fearful of language which might be interpreted as requiring them in any way to force their private sectors to transfer technology (including biotechnology).* […] "*Paragraph 1 sets the obligation for each Contracting Party to undertake "to provide and/or facilitate access for and transfer to other Contracting Parties" of: 1. technologies relevant to the conservation of biological diversity; 2. technologies relevant to the sustainable use of its components; or 3. technologies that make use of genetic resources. These technologies must not cause significant damage to the environment."*[275]

In conclusion, CBD recognizes an obligation of the contracting parties to provide and/or facilitate access for and transfer to other Contracting Parties of technologies that are relevant to the conservation and sustainable use of biological diversity (unfortunately, CBD deals solely with biotech). These technologies must not cause significant damage to the environment – that is mostly the case with biotechnology. However, CBD does not elaborate on what the "significant damage" is, or to be more accurate, what is the threshold to classify damage as significant.

Contracting parties have obligations to provide (or facilitate) access for and transfer to the other parties of technologies relevant to biodiversity protection – especially towards the developing countries. The huge financial difference between "north and south" countries was one of the drivers during the negotiations of CBD. Unfortunately, it still did not change. We are detecting more and more rapid decline in biodiversity, while most of the "megadiverse" locations are in developing countries. It seems technology transfer and financial mechanisms regulated by CBD are not quite effective. It is a simple fact, and even CBD contracting parties and specific bodies realize that. In the decision of the Conference of contracting parties from December 2022 is stated (although in a more general sense, not just technological one) that *"the lack of adequate means of implementation has been a persistent obstacle to the implementation of the Convention and of the Strategic Plan for Biodiversity 2011–2020 in developing country Parties, thus highlighting the need for enhanced international cooperation."*[276] Also, there is a specific goal in Kunming-Montreal Global biodiversity framework from 2022, based on which *"adequate means of implementation, including financial resources, capacity-building, technical and scientific cooperation, and access to and transfer of technology to fully implement the Kunming-Montreal global biodiversity*

---

[274] *„Each Contracting Party, recognizing that technology includes biotechnology, and that both access to and transfer of technology among Contracting Parties are essential elements for the attainment of the objectives of this Convention, undertakes subject to the provisions of this Article to provide and/or facilitate access for and transfer to other Contracting Parties of technologies that are relevant to the conservation and sustainable use of biological diversity or make use of genetic resources and do not cause significant damage to the environment."*

[275] Glowka L, Burhenne-Guilmin F et al, *A Guide to the Convention on Biological Diversity* (IUCN, 1994), p. 84.

[276] Decision adopted by the Conference of the Parties to the Convention on Biological Diversity (CBD/COP/DEC/15/3) accessed 19 December 2022.

framework are secured and equitably accessible to all Parties, especially developing countries, in particular, the least developed countries and small island developing States […]"[277]

As we mentioned earlier, one of the biggest constraints are limited funding, upfront costs, maintenance costs, and development funding (and that is a global problem, not just in developing countries).[278] So, the whole financial mechanism and processes adopted by CBD lack sufficient efficiency. Kunming-Montreal Global biodiversity framework confirms these words by so-called "Goal D": *"Adequate means of implementation, including financial resources, capacity-building, technical and scientific cooperation, and access to and transfer of technology to fully implement the Kunming-Montreal global biodiversity framework […] progressively closing the biodiversity finance gap of 700 billion dollars per year, and aligning financial flows with the Kunming-Montreal Global Biodiversity Framework and the 2050 Vision for Biodiversity."*[279]

When it comes to biotechnology, its dangerous nature demand adequate measures. For example, The Ad Hoc Technical Expert Group on Synthetic Biology issued a report in 2019 noting that the detectability of single nucleotide or small genomic changes could pose further challenges for some countries. Furthermore, some noted there is a lack of appropriate tools for performing risk assessment to address the specific challenges from some organisms, products, and components of synthetic biology.[280] CBD itself does regulate it only in a general manner. CBD set certain rules in Article 14 regarding environmental impact assessment and minimizing adverse impacts.[281] What diminishes its effectiveness, is the language, that has been used. Contracting parties are obliged, but only *"as far as possible and appropriate."*[282]

The issue of biotechnology is regulated in more detail in the Cartagena Protocol on Biosafety. As the introduction of the Protocol states, it has been hailed as a significant step forward in that it provides an international regulatory framework to reconcile the respective needs of trade and environmental protection concerning a rapidly growing global (biotechnology) industry.[283] Generally, the Protocol is considered a success regarding biosafety. Last, but not least, it is necessary to positively evaluate the emphasis

---

[277] Draft decision submitted by the President: Kunming-Montreal Global biodiversity framework (CBD/COP/15/L.25) accessed 18 December 2022.

[278] Speaker T, O'Donnell S, Wittemyer G et al, 'A Global Community-Sourced Assessment of the State of Conservation Technology' (2022) 36(3) *Conserv Biol* 13871.

[279] Draft decision submitted by the President: Kunming-Montreal Global biodiversity framework (CBD/COP/15/L.25) accessed 18 December 2022.

[280] 'A Global Community-Sourced Assessment of the State of Conservation Technology'.

[281] Convention on Biological Diversity, June 5, 1982, reprinted in 31 ILM 822 (1992).

[282] CBD deals with biosafety also for example in Article 8(g) and 19(3): *"Each Contracting Party shall, as far as possible and as appropriate: Establish or maintain means to regulate, manage or control the risks associated with the use and release of living modified organisms resulting from biotechnology which are likely to have adverse environmental impacts that could affect the conservation and sustainable use of biological diversity, taking also into account the risks to human health; […] The Parties shall consider the need for and modalities of a protocol setting out appropriate procedures, including, in particular, advance informed agreement, in the field of the safe transfer, handling and use of any living modified organism resulting from biotechnology that may have adverse effect on the conservation and sustainable use of biological diversity."*

[283] Cartagena Protocol on Biosafety to the Convention on Biological Diversity (2000), Montreal, 29 January 2000 (Introduction).

of the Protocol on the precautionary principle[284] (it made it much harder to deny its customary character).[285]

On the other hand, as the Ad Hoc Technical Expert Group on Synthetic Biology (to Convention on Biological Diversity) implies, there has been identified the lack of control strategies for engineered gene drives, including those with a greater potential for transboundary movement, as well as the lack of traceability and detectability methods for certain genome edited organisms and products thereof.[286]

3.2 The High Sea Treaty

The High Sea Treaty (hereinafter also as "HST") is a brand-new addition to the family of international environmental treaties. Although it has not yet entered into force[287], it is considered a huge milestone regarding biodiversity protection. It has been said that the Treaty is necessary to fulfill the commitment of the already mentioned Kunming-Montreal Global Biodiversity Framework concerning the protection of 30% of the world's oceans by 2030.[288] But does it regulate the issue of technology in relation to biodiversity protection? Firstly, we need to look at definitions.

Fortunately, HST uses the same definition of biotechnology as the CBD does. But in terms of the technology itself, HST offers a redemption to the definition of technology, and it defines "marine technology" that includes*, "inter alia, information, and data, provided in a user-friendly format, on marine sciences and related marine operations and services; manuals, guidelines, criteria, standards, and reference materials; sampling and methodology equipment; observation facilities and equipment for in situ and laboratory observations, analysis and experimentation; computer and computer software, including models and modelling techniques; related biotechnology; and expertise, knowledge, skills, technical, scientific and legal know-how and analytical methods related to the conservation and sustainable use of marine biological diversity."*[289]

Previously, we criticized the "technology" definition of CBD for it did not define anything at all, and its meaning had to be interpreted in relation to other provisions of CBD. When it comes to the definition of "marine technology," it is exactly what the CBD definition of "technology" lacks. HST adequately specifies what falls under the definition of "marine technology." Of course, it is not exhaustive, but demonstrative enumeration.

---

[284] Emphasis on the principle is a part of the objective of the Protocol.

[285] Cosbey A and Burgiel S, 'The Cartagena Protocol on Biosafety: An Analysis of Results' (*International Institute for Sustainable Development*, 2000), p. 6.

[286] Report of the Ad Hoc Technical Expert Group on Synthetic Biology (CBD/SYNBIO/AHTEG/2019/1/3). Montreal, Canada, 4-7 June 2019.

[287] „In accordance with article 68(1) agreement shall enter into force 120 days after the date of deposit of the sixtieth instrument of ratification, approval, acceptance or accession".

[288] Alberts EC, 'Seventy-plus nations sign historic high seas treaty, paving way for ratification' (*Mongabay*, 22 September 2023) <https://news.mongabay.com/2023/09/seventy-plus-nations-sign-historic-high-seas-treaty-paving-way-for-ratification/> accessed 2 November 2023.

[289] Agreement under the United Nations Convention on the Law of the Sea on the conservation and sustainable use of marine biological diversity in areas beyond national jurisdiction, 19 June 2023. (A/CONF.232/2023/4*), New York (2023).

The HST emphasizes the necessity of cooperation of the parties in the development and transfer of marine technology.[290] The treaty requires the parties to conduct an environmental impact assessment when a planned activity may have more than a minor or transitory effect on the marine environment, or the effects of the activity are unknown or poorly understood. When conducting an environmental impact assessment, the party shall consider, *inter alia, the* type of technology used for the activity and how it is to be conducted.[291]

The HST deals with technology in a quite exhaustive way. It focuses on technology from two different perspectives, capacity-building, and transfer of marine technology.[292] It emphasizes international cooperation aimed at supporting developing States Parties, in particular the least developed countries, landlocked developing countries, geographically disadvantaged States, small island developing States, coastal African States, archipelagic States, and developing middle-income countries.[293] It lists various types of capacity-building and transfer of marine technology, where we can, for example, find: The sharing of marine scientific and technological knowledge; Education and training in technology, and the application of marine science and technology, development of scientific and research capacities; Technology standards and rules etc.[294]

The HST also builds its own institutional structures. In relation to the technology, it is Capacity-building and transfer of the marine technology committee. Its main task shall be to monitor and review capacity-building and the transfer of marine technology undertaken in accordance with the HTS. Another institutional body will be the Scientific and Technical Body.[295] Same as the CBD, the HST also anchors the question of funding and relevant financial mechanisms.

In conclusion, the fact that HST addresses the biggest challenges we mentioned in the beginning such as inadequate capacity-building, lack of funding, and financial support, must be viewed as a step towards successful protection of biodiversity. In contrast with the CBD, The High Sea Treaty explicitly (and in a quite exhaustive manner) deals with capacity-building. Another plus is a language that has been used. HST uses more strict language than CBD (e.g. instead of "*should*" it uses "*shall*") A question mark should be placed above the issue of funding and financial mechanisms. For instance, although CBD also regulates this issue, its efficiency has not been sufficient enough so far.

The severity of the current situation and the interest of the international community regarding environmental protection might ensure that the HST will be a successful tool in fighting biodiversity loss. We already can see attempts to help with its implementation (although it is not yet in force). For example, in September 2023, IUCN and Allen Institute for AI teamed up to equip governmental and non-governmental organizations with advanced AI tech to protect oceans in order to speed

[290] Ibid., Art. 8.

[291] Ibid., Art. 30.

[292] Ibid., Art. 40–46.

[293] Ibid.

[294] Ibid., Annex II.

[295] Ibid., Art. 49.

up the implementation of the HST. They will also provide developing countries with access to the specific software[296] able to support implementation. IUCN will provide them technical assistance, capacity-building and policy advice.[297] It is a great example of how important are not just contracting parties (States), but also other actors, such as IUCN, or other non-governmental subjects.

4. Common provisions

As we mentioned earlier, there is one issue with monitoring technologies (drones, camera traps, etc.) that is not present anywhere else – data protection. None of the existing international environmental treaties has established adequate privacy policies regarding personal data protection. But on the other hand, it is not something that could not be regulated by some different legislative tool. There were attempts to create soft law tools, such as *Principles for the socially responsible use of conservation monitoring technology and data* (2021),[298] and *Ethical code of conduct for camera traps in wildlife research* (2020).[299] In European Union there is, of course, General Data Protection Regulation.

Although the Convention on Biological Diversity and the High Sea Treaty are not the only treaties regulating the protection of biodiversity, other treaties do not deal with technology explicitly. There are many treaties, that deal with the protection of specific localities or species, such as the Ramsar Convention, Bonn Convention, or Bern Convention. All of these treaties emphasize the necessity of cooperation and information (data) sharing (for example Article 4(3) of the Ramsar Convention).[300] Also, since they regulate the protection of specific localities (wetlands) or species (migratory species), it is necessary to ensure adequate monitoring. Technology plays an integral part in these activities, and accentuation of its importance might help, for example, to boost technological development.

To be fair, international law is not capable of regulating every possible question related to biodiversity protection. Since there are many actors and many possible contracting parties, the wording of any treaty will always be a product of compromise. Also, there are international customary rules to help with the protection of biodiversity. But if we add technology to the equation, the applicability of customary rules will be

---

296 *"Skylight (name of the software), which is used by over 300 organisations in nearly 70 countries, combines satellite technology and AI to deliver automated monitoring and detection capabilities to assist in tackling illegal, unreported and unregulated (IUU) fishing. With the ability to process and analyse millions of data points daily, the platform also provides policymakers and MPA managers with near real-time and historical intelligence to inform conservation actions."* 'IUCN and AI2 to provide AI technology at no cost to fast-track implementation of newly signed UN High Seas Treaty' (IUCN, 21 September 2023).

297 'IUCN and AI2 to provide AI technology at no cost to fast-track implementation of newly signed UN High Seas Treaty' (*IUCN*, 21 September 2023) <https://www.iucn.org/press-release/202309/iucn-and-ai2-provide-ai-technology-no-cost-fast-track-implementation-newly> accessed 5 December 2023.

298 Sandbrook C, Clark D, Toivonen T et al, 'Principles for the socially responsible use of conservation monitoring technology and data' (2021) 3 *Conservation Science and Practice* 374.

299 Sharma K, Fiechter M, George T et al. 'Conservation and people: Towards an ethical code of conduct for the use of camera traps in wildlife research' (2020) 1 *Ecol Solut Evidence* 12033.

300 Convention on Wetlands of International Importance (known as Ramsar Convention), 2 February 1971, reprinted in 996 UNTS 245.

mostly related to the biotechnology. It includes customary rules such as precautionary principle, polluter pays principle, environmental impact assessment, or responsibility of States not to cause damage to areas outside State jurisdiction.

Conclusion

Numbers have shown that biodiversity loss is even greater than we originally thought. The situation is also being called the sixth massive extinction and must be properly addressed, *inter alia,* by international law. On the other side, more and more advanced technologies are being produced each year. Unfortunately, it does not always go hand in hand with biodiversity protection. Many conservationists claim insufficient funding, lack of data sharing, and capacity-building are the biggest constraints that need to be dealt with before we can adequately use technology for biodiversity protection. After analyzing relevant international environmental treaty law (HTS was also considered although it has not yet entered into force), it is fair to say that regulation of the technology-biodiversity relationship is not as bad, as the paper might suggest. There are many issues with it (sometimes insufficient definitions or too benevolent language), but besides these issues, it properly regulates this question. The biggest issue is its application, implementation and efficiency. We consider The High Sea Treaty a stronger and more potent successor of the Convention on Biological Diversity (although its objectives are narrower), so it will be interesting to see whether it strengthens biodiversity protection, or it will be yet another failure of the international community.

3.3 Can I Have It or Not? The non-appropriation Principle in Article 2 of the Outer Space Treaty

By ***Charles Ross Bird*** (Charles University)

Introduction

Often times there is criticism of the law that it cannot keep up with technology and that law makers must create law in order to control new technology or the situations that stem from them. This frustrating sentiment was expressed by a senior member of the Government Communications Headquarters, an intelligence and security organization that oversees information of the government and armed forces of the UK, when an unauthorized usage of the their data base by an employee was discovered and could not be exposed due to the current law "I have arrived at the point at which I either make my concerns public, which means breaking the Official Secrets Act, or I fail to discharge my responsibilities to account for actions which I believe would be considered unacceptable by the general public were it aware of them."[301]

Today, the frenzy over Generative AI and how to control it stands out most in my mind.[302] Technology in space law, specifically in relation to space resources, is in my opinion the inverse. There is a massive amount of capital waiting to be invested but due to the risks involved the industry is waiting for law makers to react and new technology is pushing them to do so at an ever-increasing rate. There are five space law treaties that comprise the core of existing international space law. The most important for the purposes of this article are the Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies and the Agreement Governing the Activities of States on the Moon and Other Celestial Bodies. Those treaties however can be seen as not relevant to today's era or even not controlling due to the limited number of parties to them. But those treaties were created at time when only states had the ability and funding to operate in space.

That has dramatically changed. New technology has both lowered the threshold of entry into this field and some private companies are worth more than some states' GDP. In place of new multilateral treaties, states have taken it upon themselves to enact their own domestic laws in an effort to keep up with these changes while simultaneously trying to adhere to existing international obligations. The purpose of this article is to examine if new national legislation and non-binding multilateral agreements, specifically in the area of space resources and their appropriation, can be seen as already adhering to or

[301] Norton-Taylor R, 'Britain's spy agencies: the only watchdog is the workforce; The law cannot keep up with technology Parliamentary scrutiny is still far too weak GCHQ employee sacked' (*The Gaudian*, March 2015). <https://go.gale.com/ps/i.do?p=ITOF&u=ull_ttda&id=GALE%7CA404992423&v=2.1&it=r&sid=summon&aty=sso%3A+shibboleth> accessed 18 December 2023.

[302] Elkins D, 'Federal Policymakers: Chasing The Runaway AI Train' (*Mondaq*, 16 October 2023) <https://www.mondaq.com/unitedstates/new-technology/1377400/federal-policymakers-chasing-the-runaway-ai-train>.

in conflict with existing international legal obligations. To begin, in Section two, I will layout the international law as it stands today. Followed by Section three, which looks at pieces of national legislation that speaks the concept of national appropriation and how the US led Artemis Accords appear to be providing a vehicle for a refined definition of what constitutes a national appropriation in international law. Section four will dissect Article 2 of the Outer Space Treaty. Specifically, it will look at the purpose of the treaty, the ordinary meaning of national appropriation, and subsequent state practice in regard to national appropriation. Lastly in Section five, I will conclude that even though the purpose of the treaty and ordinary meaning of national appropriation was to prevent the militarization of space and that the wording of it only applied to states respectively, the subsequent state practice does not yet exist to definitely say that national appropriation does not apply to non-state actors.

1. Current State of International Law

At present, the most authoritative document controlling the law of outer space is the Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies.[303] Being a mouthful, it is more commonly known as the Outer Space Treaty (OST). There are four other treaties comprising the core treaty documents of the law of outer space.[304] However, as time progressed and more state interests in outer space became apparent, fewer and fewer states agreed to be bound by these types of treaties. This is very apparent when you examine the state parties to the youngest treaty in this group, the Agreement Governing the Activities of States on the Moon and Other Celestial Bodies (Moon Agreement),[305] which currently stands at eighteen,[306] none of which are major space powers. To further emphasize this point, Saudi Arabia officially gave notice to withdraw from the treaty on 5 January 2023, which takes effect on 5 January 2024.[307] Even though there have not been any multinational treaties on outer space concluded since the Moon Agreement, commercial interests and states have not been sitting idly by. There is a simple yet powerful motivating force that is driving the development in this area: money.

Lloyd's of London predicts that by 2040, the global space market will be valued at one trillion US dollars ($ 1,000,000,000,000).[308] Space mining itself has a projected value of roughly seven and half billion US dollars by 2033.[309] In press releases,

[303] Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies (1967).

[304] Outer Space Treaty (1967) (114 States Parties), The Rescue Agreement (1968) (98 States Parties), The Liability Convention (1972) (98 States Parties), The Registration Convention (1975) (75 States Parties), and The Moon Agreement (1979) (18 States Parties).

[305] Agreement Governing the Activities of States on the Moon and Other Celestial Bodies (1979).

[306] United Nations Office for Disarmament Affairs Treaties Database, available at https://treaties.unoda.org/t/moon/participants?status=parties.

[307] U.N., C.N.4.2023. TREATIES-XXIV.2 (Depositary Notification).

[308] Sheehan M, 'Lloyd's of London launches space insurance policy' *Reinsurance News* (4 December 2019) <https://www.reinsurancene.ws/lloyds-of-london-launches-space-insurance-policy/> accessed 4 November 2023.

[309] Market forecast by Fact.MR analyzing more than 30 countries' space mining markets. <https://www.factmr.com/report/space-mining-market> accessed 2 November 2023

forecasts, studies, and journal articles the common thread of lower barriers of entry and advancement in technology are referred to as the main drivers of this expected growth. A huge limitation to this growth in the area of space resources is ownership of those resources and how they can be used. Article 2 of the OST reads "Outer space, including the Moon and other celestial bodies, is not subject to *national appropriation* by claim of sovereignty, by means of use or occupation, or by any other means." I doubt that in 1967, the drafters of the OST could have imagined those thirty words to be such an obstacle today.

2. Current National Legislation and Policies

States have begun to address the issue with domestic legislation in absence of any new hard international law on the topic. In 2015, the United States enacted the US Commercial Space Launch Competitiveness Act, sometimes known as the Spurring Private Aerospace Competitiveness and Entrepreneurship Act (Competitiveness Act).[310] Part of that broadly scoped act seeks to address the issue of national appropriation by stating;

> *A United States citizen engaged in commercial recovery of an asteroid resource or a space resource under this chapter shall be entitled to any asteroid resource or space resource obtained, including to possess, own, transport, use, and sell the asteroid resource or space resource obtained in accordance with applicable law, including the international obligations of the United States.*[311]

This was not without criticism though. An earlier attempt aimed specifically at space resources was H.R. 1508, titled 'Space Resource Exploration and Utilization Act of 2015'.[312] While H.R. 1508 was being debated in Committee, Prof. Joanne Gabrynowicz from the University of Mississippi penned a letter to the ranking member voicing serious concerns that the proposed bill appeared to be in conflict with the U.N. Outer Space Treaty, irregardless of the phrase "consistent with the existing international obligations of the United States",[313] which is now codified into law as "… obtained in accordance with applicable law, including the international obligations of the United States".[314] Be that as it may, the enactment of the Competitiveness Act broke the figurative dam. Shortly thereafter, Luxembourg enacted legislation specifically allowing space resources to be owned,[315] followed by the UAE in 2019[316] and Japan in 2021.[317]

---

310 H.R. 2262, 114th Cong. (2015) (enacted) (Competitiveness Act).

311 51 U.S.C. § 51303 (2015).

312 <https://www.govinfo.gov/content/pkg/BILLS-114hr1508ih/pdf/BILLS-114hr1508ih.pdf> accessed 4 November 2023.

313 H.R 1508, 114th Cong. at 20 (Minority Views) (2015). Even though H.R. 1508 died in committee due to the end of the Congressional session, the text was consolidated into the Competitiveness Act.

314 See (n 311).

315 *Loi du 20 juillet 2017 sur l'exploration et l'utilisation des ressources de l'espace*, Luxembourg (2017).

316 *Federal Law On the Regulation of the Space Sector (No.12)*, UAE (2019).

317 *Act on Promotion of Business Activities Related to the Exploration and Development of Space Resources Act No. 83*, Japan (2021).

Piggy backing off of the Competitiveness Act, in 2020, the United States launched the Artemis Accords.[318] When the Accords were initially launched there were 8 members to the Accords, Luxembourg, the UAE, and Japan being among them.[319] As of the time of this writing there are 31 members.[320] The United States Artemis Accords in based in the OST but also as principles to guide the 21st century of space exploration.[321] In the Accords, among other provisions, speak to the extraction of space resources and the agreement by members that said extraction does not constitute an appropriation under the Article 2 of the OST.[322] The debate for the purposes of this article goes back to those thirty words and whether or not parties to the OST can square the circle between honoring Article 2 regarding non-appropriation and their domestic legislation. To do that, Article 2 needs to be examined more closely.

3. Interpretation of Article 2 of the OST

The starting point for clarifying treaties and their provisions is the Vienna Convention on the Law of Treaties (VCLT).[323] The VCLT is considered customary international law which the International Court of Justice recognized in the 1994 *Libya/Chad* case.[324] This following analysis will look at the purpose, ordinary meaning, and state practice as the means of interpreting Article 2 of the OST. Article 31(2) spells out the process of interpretation of the purpose of a treaty. Article 31(1) of the VCLT states "A treaty shall be interpreted in good faith in accordance with the ordinary meaning to be given to the terms of the treaty in their context and in the light of its object and purpose" and Article 31(3)(b) also allows treaties to be interpreted by examining state practice subsequent to the conclusion of the treaty.

a) The Purpose of the Treaty

The purposes of the OST can be derived from examining the documents submitted by the parties prior to completion of the treaty along with knowledge of the events at the time and by examining the preamble. The OST was seen as a needed bulkhead during the Cold War when the two nuclear superpowers, the USSR and the United States, were beginning to extend their influence into outer space. This can be seen in the initial letters between the United States and the USSR emphasizing the need for peaceful and joint cooperation in space and the desire to keep weapons from being used and placed there.[325] These ideas then made it into the preamble of the OST by recognizing the common interests of human kind, the exploration and the use for peaceful purposes,

---

318 'The Artemis Plan, NASA's Lunar Exploration Program Overview' (September 2020) <https://www.nasa.gov/sites/default/files/atoms/files/artemis_plan-20200921.pdf> accessed 4 November 2023, p. 8.

319 Ibid.

320 Accords homepage, <https://www.nasa.gov/artemis-accords/> accessed 5 November 2023.

321 <https://www.state.gov/artemis-accords/> accessed 5 November 2023.

322 The Artemis Accords Principles for Cooperation in the Civil Exploration and Use of the Moon, Mars, Comets, and Asteroids for Peaceful Purposes (2020), para 10.

323 Vienna Convention on the law of Treaties (1969), vol. 1155.

324 ICJ *Territorial Dispute Libyan Arab Jamahiriya/Chad*, Judgement [1994] ICJ Rep 1994.

325 U.N. Doc. A/AC.105/C.2/L.12 (USA) and U.N. Doc. A/AC.105/C.2/L.13 (USSR).

and the specific reference to Resolution 1884 (XVIII) calling on the prohibition of placing nuclear or other weapons of mass destruction in orbit or on celestial bodies.[326] Deconflicting space by preventing it from becoming another battlefield and the belief that outer space was for all humankind to be used and explored peacefully was the main concern for the drafters. It would be fair to say that commercial interests were not the focus of those debates as that by its very nature is not for the public at large. Further evidence that the treaty's purpose is that the treaty itself is housed in the U.N Office for Disarmament Affairs Treaties Database.[327] Although, I would be remiss if I didn't add that the French delegation did vocalize the possibility of extracting minerals as a use of outer space if that was ever to become possible.[328] How fortuitous of them.

b) The Ordinary Meaning of National Appropriation

The current sticking point I will be focusing on in regard to vocabulary revolves around the terms, *national appropriation* in Article 2 of the OST. Black's Law dictionary defines 'national' when used as an adjective, which is the usage here, as "of or relating to a nation"[329] and an 'appropriation' as "the exercise of control over property; a taking of possession."[330] By these definitions it would appear that a national appropriation must involve some kind of property owned or possessed by a nation. Gorove, who is considered a pioneer in space law, comes to this very conclusion in his analysis of Article 2 when he said that "the treaty in its present form appears to contain no prohibition regarding individual appropriation or acquisition by a private association or an international organization."[331] Additionally, there is some recent US case law that further buttresses the point that a national appropriation can only occur when the US Congress has authority over the purchase of or financial control of said property.[332] Lee, in his article on the Article 2 regarding sovereignty and private actors, found that the official Chinese text of the OST was very specific in limiting the prohibition of appropriation against states only and that since it was an official text it should be used for interpretative purposes in that an appropriation only prohibits states.[333] The ordinary meaning of national appropriation must include the government directly taking the property or in this case the resources. With that in mind, let's move to the subsequent practice of the states parties that in my opinion adds clarity to the provision rather than violate it.

---

326 U.N. Doc. A/RES/1884(XVIII).

327 U.N Office for Disarmament Affairs Treaties Database, < https://treaties.unoda.org/treaties> accessed 4 November 2023.

328 U.N. Doc. A/AC.105/C.2/SR.63.

329 *Black's Law Dictionary 1050* (Bryan A. Garner ed., 8th ed., West, 2004).

330 Ibid., p. 110.

331 Gorove S, 'Interpreting Article II of the Outer Space Treaty' (1969) 37 *Fordham L. Rev.* 349.

332 *Collins et. al. v The United States of America, 2005 WL 946896 (N.D. Ill. Apr. 19, 2005).*

333 Lee RJ, 'Article II of the Outer Space Treaty: Prohibition of State Sovereignty, Private Property Rights, or Both' (2004) 11 *Austl. INT'L L.J.* 128, p. 130.

c) Subsequent Practice of States

As previously mentioned, the VCLT allows interpretation of treaty provisions by analyzing the actions and behaviors of states after they conclude a treaty. Or, as Buga phrased it, continuing treaty negotiations by other means.[334] To assess subsequent practice, two elements need to be addressed. The first is the behavior while executing a treaty and the agreements between the parties coming from that behavior.[335] To examine the behavior of the subsequent practice there needs to be a determination if the parties have taken a position in regard to the interpretation of the treaty.[336] Deplano, in my opinion, correctly applies the definition of *modus vivendi* provided by the ILC to in her analysis of the 8 states that had signed on to the Accords at the time of her writing. That being an agreement to take a position is not a position in itself.[337] However, I would argue that there have been some changes since that writing that can be seen as an objective position by one new member, Saudi Arabia. As mention previously, Saudi Arabia officially invoked their desire to formally withdraw from the Moon Agreement.[338] However, six months before that invocation, Saudi Arabia became a member of the Artemis Accords.[339] I find this significant because there is a large difference in provisions regarding space resources in the Moon Agreement compared with the Artemis Accords. Article 11 of the Moon Agreement not only established that the Moon is the common heritage of mankind[340] and roughly restates the OST's Article2 that "the Moon is not subject to national appropriation by any claim of sovereignty, by means of use or occupation, or by any other means" in Article 11(2). However, Article 11(3) is very precise in its definition of who can and cannot appropriate those resources. It states that "neither the surface nor the subsurface of the Moon, nor any part thereof or natural resources in place, shall become property of any State, international intergovernmental or non-governmental organization, national organization or non-governmental entity or of any natural person . . ."[341] When Article 11(3) is contrasted with Section 10 of the Accords that explicitly states that mining those same resources does not constitute an appropriation,[342] it is easy to see that they are mutually exclusive. In my view, Saudi Arabia's choice to formally withdraw from the Moon Agreement in favour of joining the Artemis Accords, is clearly an objectively visible position in regard to the ILC's definition of *modus vivendi*. That is the behavior of only one member

---

334 Buga I, 'The Impact of Subsequent Customary International Law on Treaties: Pushing the Boundaries of Interpretation' (2022) 69 *Netherlands International Law Review* 241, p. 242.

335 Deplano R, 'The Artemis Accords: Evolution or Revolution in International Space Law' (2021) 70 *ICLQ* 799, p. 806.

336 Deplano R, 'The Artemis Accords: Evolution or Revolution in International Space Law' (2021) 70 *ICLQ* 799, p. 806, citing ILC, 'Report of the International Law Commission on the Work of its Seventieth Session', p. 43.

337 ILC, 'Report of the International Law Commission on the Work of its Seventieth Session', p. 43.

338 Supra, (n 306).

339 US Department of Sate Press Release (16 July 2022), <https://www.state.gov/kingdom-of-saudi-arabia-signs-the-artemis-accords/> accessed 4 November 2023.

340 *Moon Agreement*, Art. 11(1).

341 Ibid., Article 11(3).

342 Supra, (n 321).

of the Accords, and Australia, Mexico, and the Netherlands are parties to the Moon Agreement while also members of the Accords. Australia has stated that it believes that there is no conflict between the Accords and the Moon Agreement.[343] The Accords are not binding instruments of international law, so they are not on equal footing with treaties like the Moon Agreement. But Saudi Arabia's withdrawal is seen as a dark omen for the Moon Agreement by some. Rightly asserting that due to the small number of parties to the Moon Agreement, any more defections to Artemis and subsequent withdrawals would be a death nail for the Moon Agreement.[344] Also notable is that the Accords proport to be in accordance with 4 out of the 5 core space treaties, the Moon Agreement notably absent from that list.[345] Perhaps the US is betting on its demise due to the low number of parties and counting on defections to the Accords. Saudi Arabia's actions aside, I have seen no other overt conduct which in my opinion would be considered as taking an official position for the purposes of identifying subsequent practices, even with the additional members. But that can quickly change in relation to the abandonment of the Moon Agreement as previously discussed. There needs to be some repetition of subsequent practices to be meaningful too according to the ILC.[346] However, the duration and frequency of those new practices only need to be long enough to allow other states to become aware and react to those practices, but that can happen in a short amount of time.[347] The second prong of the subsequent practices test, agreements stemming from conduct, is quite straight forward. Section 10(2) of the Accords states that: "*The Signatories affirm* that the extraction of space resources does not inherently constitute national appropriation under Article II of the Outer Space Treaty…" This is clearly an agreement from the members that is commonly understood for the purposes of the VCLT.[348] It is important to note that the Russian space agency Roscommon compared President Trump's 2020 order encouraging citizens to mine the Moon commercial purposes as policy colonialism.[349] However, Sergey Saveliev, the deputy general director for international cooperation at Roscommon, made the point that since the United States were not a party to the Moon Agreement they should be able to use and explore space resources in accordance with international law.[350] But if Russia wishes to establish their own base on the Moon,[351] they will need the resources

[343] Australian Space Agency Letter to the 60th UNOOSA Legal Subcommittee <https://www.unoosa.org/documents/pdf/copuos/lsc/2021/statements/item_14_Australia_ver.1_4_June_PM.pdf>.

[344] Wedenig S and Nelson JW, 'The Moon Agreement: Hanging by a Thread?' (*McGill Institute of Air and Space Law*, 26 January 2023) <https://www.mcgill.ca/iasl/article/moon-agreement-hanging-thread>.

[345] *Artemis Accords*, preamble.

[346] Supra, (n 333).

[347] *ICJ North Sea Continental Self (Federal Republic of Germany/Denmark; Federal Republic of Germany/Netherlands)*, Judgement [1969] ICJ Rep 1969, p. 3, para 74.

[348] VCLT 31(3)(b).

[349] Daemmrich B, 'Russia Compares Trump's Space Mining Order to Colonialism' (*The Moscow Times*, 7 April 2020) <https://www.themoscowtimes.com/2020/04/07/russia-compares-trumps-space-mining-order-to-colonialism-a69901> accessed 4 November 2023.

[350] Jamasmie C, 'Russia slams Trump's order to spur mining on the moon' (*Mining. com*, 9 April 2020) <https://www.mining.com/russia-slams-trumps-order-to-spur-mining-the-moon-asteroids/>. accessed 4 November 2023.

[351] Moskva News Agency, 'Russia Plans Long-Term Base on the Moon-Space Agency' *The Moscow Times*

there just as much as the Artemis members. It will be interesting how they approach this issue in the future. Even though, the Accords now have 31 members, one of whom I believe has staked a position on the national appropriation provision in the OST that would fit the ILC's definition of *modus vivendi* and all the members have signaled a common understanding of those provisions. I do not think it rises to the level to be considered a subsequent practice just yet. The key word being yet.

Conclusion

There is very convincing evidence that the original drafters' primary purpose of the Ost was to prevent the militarization of outer space by the nuclear capable superpowers at the time and that the OST never intended to apply the non-appropriation principle found in Article 2 of the OST to anything other than states under a plain reading of the treaty provision. However, I do not think that the argument that subsequent practice has also provided the same interpretation of those provisions just yet. In my opinion it is only a matter of time before we see actual state practice that will establish *modus vivendi*. At this point it appears that the members of the Accords have done what they can to legally facilitate the commercial mining of space resources. Now we just need to wait for technology to catch up. We will need to wait to see what comes next and who does what.

A legal take away from an article in Space News shows the inevitable direction this is travelling however. In 2020, NASA solicited bids from multiple different companies to go to the moon, extract 50-500g samples, and once the companies could prove they have acquired those samples, NASA would pay them a nominal fee of between $15,000 to $25,000. The company would leave the sample on the Moon to be collected later. NASA explained that they were buying the lunar soil to demonstrate that it could be done, and to establish a behavior that was in compliance with the Outer Space Treaty. In the comments at the end of the article, a commenter claimed that they didn't see putting samples of that soil in containers just to sit on the moon and do nothing as more than a stunt. The immediate and only response was "You must not be a Lawyer."[352]

(Moscow, 6 November 2018) <https://www.themoscowtimes.com/2018/11/06/russia-plans-long-term-base-on-moon-space-agency-a63406> accessed 4 November 2023.

[352] Foust J, 'NASA offers to buy lunar samples to set space resources precedent' (*SpaceNews*, 10 September 2020) <https://spacenews.com/nasa-offers-to-buy-lunar-samples-to-set-space-resources-precedent/> accessed 4 November 2023.

CHAPTER IV

REGION-SPECIFIC ISSUES

4.1 Tax and Technology in Developing Countries

By ***Pavlína Krausová*** (Charles University)

Introduction

The purpose of this article is to examine the intricate relationship between technology and taxation in developing countries, focusing on the administrative and legal challenges and underscoring the importance of international collaboration. It delves into the specific circumstances of these countries, addressing key issues such as tax administration, technological adoption, and data management. This encompasses challenges in enforcing tax compliance, the difficulties of implementing international tax standards, and the potential of information technology in tax collection and analysis.

Supplemented with specific examples and studies, the article will provide insights into both the problems and prospects of integrating tax and technology in developing countries. It aims to demonstrate how technological innovations can enhance tax compliance and expand the tax base, while also acknowledging the associated challenges of data protection, legal clarity, and maintaining equity in a digital society.

The first part of the article focuses on the use of new technologies, including the digitization of tax systems, big data and analytics, and the application of blockchain technology. Each section will offer extensive examples from various countries, showcasing the diverse impact and potential of technology in improving tax systems. The second part concentrates on international cooperation, exploring how global tax policies and information exchange norms impact developing countries. It will evaluate the challenges and opportunities presented by international initiatives and standards, highlighting the crucial need for capacity building and support from international bodies. Finally, the article will discuss the development and protection of taxpayer rights in the context of technological advancements. It will emphasize the significance of data security, privacy concerns, and equitable access to technology, underlining the necessity for continued research, policy innovation, and international collaboration in this rapidly evolving field.

1. Preliminary Remarks

1.1 Scope of the Term Developing Country

Although the term *developing country* is extensively used in the international community, no globally agreed definition exists. Various organizations and institutions[353] define developing countries using a variety of criteria, including income, economic development, industrialization, standard of living, and other socioeconomic aspects.

[353] For example the United Nations and the United Nations Conference on Trade and Development, the World Bank, the Organisation for Economic Co-operation and Development, or the International Monetary Fund.

By looking at the similarities and differences, it's evident that the term serves different functions for different international bodies, and the purpose may be for example analytical, a policy formulation or an aid allocation.

For example, in the United Nations system, there is no official definition distinguishing developing and developed countries or areas. Initially, these categories were created for statistical ease. In December 2021, following discussions with various international statistical organizations, the UN removed the categories. This flexibility acknowledges that the classification as a developed or developing region is often a sovereign decision of a state.[354] The UN also recognizes the designation of *least Developed Countries* (LDCs) based on criteria that include low income, weak human assets, and economic vulnerability.[355]

When choosing specific examples of technology implementation in tax administration, this article has not followed one specific definition but rather considered a broader context of the country development and a value of the data available.

1.2 Specific Situation of Developing Countries

Both developing and developed countries have tax, technological, and data management concerns, however developing countries may struggle with basic functions like audits and tax collection, which are exacerbated by international tax standards and digital taxes.[356] Such governments often find it difficult to enforce tax compliance, in part because they do not have accurate records of taxpayer earnings.[357] While issues such as privacy or corruption are common to both developing and developed countries, they differ in relative importance.[358] Currently, states have a significant opportunity to leap forward to advanced technology-based systems, which can result in increased revenue and tax base expansion, more effective resource use, and the ability to complete more risk assessments using more sophisticated tools.[359] However, while digital solutions can streamline processes, they demand higher skills for effective management. Lack of ability on the taxpayer side is also a concern, particularly in developing countries, resulting in low levels of compliance, particularly with more complex instruments like VAT. A choice of how to allocate scarce resources needs to

---

354 UN Statistics Division, *Methodology. Standard Country or Area Codes for Statistical Use* (M49), <https://unstats.un.org/unsd/methodology/m49> accessed 20 October 2023.

355 UN Department of Economic and Social Affairs, *About Secretariat of the Committee for Development Policy* <https://www.un.org/development/desa/dpad/about-us/secretariat-of-the-committee-for-development-policy.html> accessed 25 October 2023.

356 Asian Development Bank, (2022), *Launching a Digital Tax Administration Transformation: What You Need to Know* (1st ed.), Asian Development Bank Institute, p. 24.

357 Ali M, Shifa AB, Shimeles A and Woldeyes F, 'Building Fiscal Capacity in Developing Countries: Evidence on the Role of Information Technology' (2021) 74(3) *National Tax Journal* 591.

358 Bird R and Zolt E, 'Technology and Taxation in Developing Countries: From Hand to Mouse' (2008) 61 *National Tax Journal* 791, p. 2.

359 OECD, 2023 Progress Report on Tax Co-operation for the 21st Century. *OECD Report for the G7 Finance Ministers and Central Bank Governors* (2023) <https://doi.org/doi:https://doi.org/10.1787/d29d0872-en>, p. 28.

be part of the cost-benefit analysis of any digital transformation program.[360] It may also be difficult to meaningfully evaluate the true state of a digitalization of specific tax administrations. Such evaluations, which are frequently undertaken by third parties such as donor agencies or non-governmental organizations, are often primarily focused on quantitative indicators, which might not accurately represent success. Furthermore, because tax administrations do not benefit directly from these exercises and are the ones being evaluated, there is a possibility that they will not submit correct data.[361]

Nonetheless, this year, the OECD has issued a progress report emphasizing that common, collaborative, digitally enabled and more real time approaches to the administration of common rules are becoming a central feature in the design of international tax rules.[362]

2. Technological Empowerment in Tax Administration

2.1 Adopting New Technologies

Currently, tax and international tax policy debates are often driven by issues such as the amount of corporate tax paid by multinational corporations and its allocation across borders. Yet, we are experiencing an important phase in the ongoing digital transformation.[363] This technological transformation imposes on the law new concepts such as the cloud, robots, artificial intelligence, algorithm, internet of things, big data, digital presence, virtual permanent establishment, significant economic presence, blockchain, bitcoin, or intelligent assistants.[364] A question for the future is *how can developing countries effectively acquire and integrate new technologies in their tax administrations to enhance efficiency and compliance, while addressing the associated legal, institutional, and capacity-building challenges*.

2.2 Digital Taxation Systems

General concept of digitalization of a tax administration primarily involves converting data and manual processes to digital and computer-supported formats, such as shifting from over-the-counter tax payments to electronic methods. It also encompasses advancing from basic digital tools to more integrated and automated processes.[365] Such new technologies may have a fueling effect on tax revenue generation linked to its ability to mitigate the challenges of delay, high administrative cost, evasion and corruption

---

[360] Asian Development Bank, (2022), *Launching a Digital Tax Administration Transformation: What You Need to Know* (1st ed.), Asian Development Bank Institute, p. 24.

[361] Vázquez-Caro J and Bird R, 'Benchmarking Tax Administrations in Developing Countries: A Systemic Approach' (2010) 9 *E Journal of Tax Research* 5, p. 6.

[362] OECD, 2023 Progress Report on Tax Co-operation for the 21st Century. *OECD Report for the G7 Finance Ministers and Central Bank Governors* (2023) <https://doi.org/doi:https://doi.org/10.1787/d29d0872-en>, p. 3.

[363] Russo R, 'Reflections about the Implications of Platforms and Technology for Taxation and Taxpayers' Rights' in Weber, D (ed), *The Implications of Online Platforms and Technology on Taxation* (IBFD, 2023), pp. 1–3.

[364] ILA, Sadowsky, M. e. c. *White Paper 12 on Taxation: Taxing the Future* (International Law Association (2023) <https://www.ilaparis2023.org/en/white-paper/taxation/>, pp. 66–67.

[365] OECD, 'Supporting the Digitalisation of Developing Country Tax Administrations' (2021), p. 143.

associated with paper-based tax procedures.[366] A study analyzing the impact of ICT[367] on revenue mobilization in the Southern African Development Community (SADC) found that particularly internet usage and mobile subscriptions significantly boosts revenue generation across 12 member countries from 2001 to 2020. The effect was more pronounced with internet usage, indicating ICT's role as a key revenue enhancer in the region.[368]

As demonstrated below, many developing countries have established or are in the process of establishing digital taxation systems. This includes tax return e-filing, e-invoicing, and digital payment platforms. Technology can significantly aid tax authorities in identifying taxable entities and assessing tax liabilities, using tools like electronic billing machines for sales transactions and data from third-party sources such as employers and financial institutions.[369]

Especially mobile technology has been harnessed for taxation services in several African countries. Taxpayers in Rwanda and Uganda, for example, can now pay taxes using mobile money services, which significantly reduces the costs and time associated with tax compliance for individuals and small businesses.[370] This overcomes challenges like inadequate postal systems and long distances to tax offices. Such service enables taxpayers to manage their data, view accounts and returns, and access information online, and can also be extended to intermediaries like tax advisors and accountants.[371] Another example may be Rwanda introducing Electronic Billing Machines as part of its efforts to improve VAT compliance and collection. These devices are used by businesses to record transactions and directly transmit sales data to the Rwanda Revenue Authority. This initiative has been effective in reducing VAT fraud and increasing revenues. [372] In Nigeria, the tax administration (FIRS) launched the TaxPro-Max platform in 2021. The platform is an online tax administration solution that allows taxpayers to register, file, and pay taxes electronically. TaxPro-Max also provides a single-view to taxpayers for all transactions with the tax administration. The FIRS has been reporting a consistent increase in revenue collection each year since the adoption of the platform.[373]

---

366 Jemiluyi OO, 'Tax Revenue Mobilization Effort in Southern African Development Community (SADC) Bloc: Does ICT Matter?' (2023) 11(1) *Cogent Economics & Finance* 1, p. 10.

367 UNESCO defines ICT as a diverse set of technological tools and resources used to transmit, store, create, share or exchange information.

368 'Tax Revenue Mobilization Effort in Southern African Development Community (SADC) Bloc: Does ICT Matter?', p. 10.

369 Okunogbe O and Santoro F, 'The Promise and Limitations of Information Technology for Tax Mobilization' (2023) 38(2) *The World Bank Research Observer* 295, p. 317.

370 GSMA, 'Paying Taxes Through Mobile Money: Initial Insights into P2G and B2G Payments' (*GSMA*, 4 December 2014) <https://www.gsma.com/mobilefordevelopment/programme/mobile-money/paying-taxes-through-mobile-money-initial-insights-into-p2g-and-b2g-payments/>.

371 KfW Development Bank, 'Information Technology in Tax Administration in Developing Countries' (*KfW*, 2015) <https://www.taxcompact.net/sites/default/files/resources/2015-07-ITC-IT-Tax-Administration.pdf>, p. 19.

372 'Mandatory e-Invoicing in Rwanda: Electronic Invoicing System (EIS)' (*Edicom,* 22 March 2023) <https://edicomgroup.com/blog/mandatory-einvoicing-rwanda-eis>.

373 Addis Tax Initiative, 'The Digital Transformation of Tax Administrations' (*ati*, 19 July 2023) <https://www.addistaxinitiative.net/news/digital-transformation-tax-administrations-0>.

A more extensive study has been conducted in Tajikistan. Using data from small and medium-sized firms in Dushanbe, according to the study, e-filing dramatically saved the time spent on tax-related operations by 40%, effectively tripling taxes paid by enterprises more likely to evade while decreasing payments by firms less likely to avoid. E-filing also resulted in fewer bribes because extortion chances were eliminated.[374] A study conducted in Peru investigated the impact of electronic invoicing reforms on tax compliance and technology adoption. It found that firms are more likely to adopt e-invoicing voluntarily if their trading partners are mandated to do so, demonstrating positive spillover effects in technology adoption.[375]

2.3 Big Data and Analytics

Big data involves processing large volumes of diverse information quickly and cost-effectively for improved knowledge, decision-making, and automation. It encompasses three key dimensions, volume, speed, and variety. Large-scale data from multiple sources is combined with sophisticated algorithms and uses methods like data mining, machine learning, and neural networks.[376]

A lot of policy discussion surrounds investments in detection capabilities, such as third-party reporting, the use of electronic databases, and technology-based tools for comprehending and tracking the tax base.[377] Some countries use datamining or machine learning systems based on artificial intelligence to support their tax audits, to identify fraud risks in an automated way, or to carry out research, investigation, programming, control and recovery operations for tax violations. In Brazil, the use of artificial intelligence and big data has allowed, even during the pandemic, to increase the Brazilian budget by 10%.[378] By evaluating massive datasets to spot irregularities, like differences in sales reporting for income tax and VAT, technology improves tax monitoring.[379] In Chile, the Servicio de Impuestos Internos (SII) employs AI tools to predict which taxpayers are most likely to underreport income, thereby optimizing their audit selection process. [380] Another recent development in Argentina demonstrates how tax authorities must adapt to taxpayer behavior. In 2022, Argentina's tax administration (AFIP) implemented the Comprehensive System for Monitoring Payments Abroad for Services (SIMPES), which has been effective in discovering

[374] Okunogbe O and Pouliquen V, 'Technology, Taxation, and Corruption: Evidence from the Introduction of Electronic Tax Filing.' (2022) 14(1) *American Economic Journal: Economic Policy* 341.

[375] Bellon M, 'Technology and Tax Compliance Spillovers: Evidence from a VAT E-Invoicing Reform in Peru' (2023) *Journal of Economic Behavior & Organization* 212, p. 756.

[376] Faúndez A, Mellado-Silva R and Aldunate-Lizana E, 'Use of Artificial Intelligence by Tax Administrations: An Analysis Regarding Taxpayers' Rights in Latin American Countries' (2020) 38 *Computer Law & Security Review* 105441, p. 3.

[377] Okunogbe O, 'Becoming Legible to the State: The Role of Identification and Collection Capacity in Taxation (English)' (*World Bank Group*, 2021) <http://documents.worldbank.org/curated/en/589171637156811373/Becoming-Legible-to-the-State-The-Role-of-Identification-and-Collection-Capacity-in-Taxation>, p. 19.

[378] ILA, Sadowsky, p. 70.

[379] 'The Promise and Limitations of Information Technology for Tax Mobilization' (2023), p. 317.

[380] 'Use of Artificial Intelligence by Tax Administrations: An Analysis Regarding Taxpayers' Rights in Latin American Countries', pp. 3–4.

unreported crypto-asset income, notoriously difficult to trace for tax purposes.[381] The final study on China's Golden Tax Project III (GTP III) revealed that the adoption of advanced information technology in tax administration significantly enhanced corporate income tax compliance. Analyzing data from 2010 to 2017, the research showed a substantial decrease in tax sheltering activities, especially among companies with higher tax rates and political connections. The effectiveness of GTP III is attributed to improved third-party information reporting and stronger tax enforcement, particularly in areas with limited tax inspection resources.[382]

2.4 Blockchain

Blockchain technology is being explored as a way to track transactions and combat VAT fraud. Through decentralized recording, blockchain technology provides significant data recording, security, and transparency.[383] Several countries have started to use blockchain technology in tax administration. An example is China's GAChain system automated company and asset registration on blockchain, secure electronic invoicing and tax collection.[384] Blockchain is also enabling new forms of collaboration, such as horizontal collaboration between tax administrations and other agencies in Brazil. Furthermore, multinational systems such as Mercosur's BConnect use blockchain to improve information flow.[385]

An interesting study conducted in Turkey investigated tax office employees' perceptions of blockchain technology in tax transactions. The findings reveal a moderately positive attitude towards incorporating blockchain-based applications, considering the technology secure against cyber threats and safe for handling taxpayers' personal data. They also view positively the idea of a blockchain wallet for taxpayers, enabling easier and cost-effective transactions without needing to visit tax offices. Additionally, the employees are moderately optimistic about future implementation of blockchain and artificial intelligence in tax offices, recognizing benefits like reduced stationery use and a seamless transition to systems like e-government. [386]

The key players in the cryptocurrency industry, originally viewed as anti-establishment, are increasingly recognizing blockchain's potential global impact.[387]

However there are new challenges ahead. The potential of blockchain technology, which the law is beginning to grasp, may soon be overtaken by the advent of the

[381] Addis Tax Initiative, 'The Digital Transformation of Tax Administrations' (*ati*, 19 July 2023) <https://www.addistaxinitiative.net/news/digital-transformation-tax-administrations-0>.

[382] Jianjun L, Xuan W and Yaping W, 'Can Government Improve Tax Compliance by Adopting Advanced Information Technology? Evidence from the Golden Tax Project III in China.' (2020) 93 *Economic Modelling* 384.

[383] Kükrer C, and Eğmir RT, 'Perception of Tax Office Employees for the Use of Blockchain Technology in Tax Office' (2019) 6(12) *International Journal of Advanced Research* 638.

[384] ILA, Sadowsky, p. 69.

[385] Ibid., pp. 69–70.

[386] Kükrer C, and Eğmir RT, 'Perception of Tax Office Employees for the Use of Blockchain Technology in Tax Office' (2019) 6(12) *International Journal of Advanced Research*, p. 648.

[387] Russo R, 'Reflections about the Implications of Platforms and Technology for Taxation and Taxpayers' Rights' in Weber, D (ed), *The Implications of Online Platforms and Technology on Taxation* (IBFD, 2023), p. 6.

quantum computer with a potential to break the cryptographic security keys securing the blockchain.[388]

2.5 COVID-19 Pandemic Response and Future Development

The COVID-19 pandemic accelerated the adoption of digital tools in various sectors, including tax administrations. As physical distancing measures were enforced, numerous tax authorities rapidly transitioned to remote operations. This health crisis also underscored the critical role of public revenue, especially in developing economies.[389] This shift towards digitalization in tax administration is likely to have lasting implications.

Despite substantial technological advances in the last 40 years, technology alone cannot provide a simple answer for improving tax policy or administration in developing nations.[390] Administrators may seek quick solutions, such as purchasing new IT systems or recruiting additional personnel,[391] but successful digitalization also requires an adaptation of work patterns and the resolution of management difficulties, needing resilience and tenacity throughout the process's various stages.[392] It is also prudent to consider that technological progress might also open fresh opportunities for tax evasion and avoidance for specific groups, particularly those with high incomes, perhaps leading to increasing economic imbalance.[393]

Finally, the challenges faced by countries in their digital transformation journeys vary based on their digital maturity. Countries in early digitalization stages primarily grapple with establishing necessary infrastructure, while those more advanced encounter issues related to data security, privacy, and confidentiality, as well as workforce training for the digital era.[394]

3. International Cooperation

3.1 Navigating Global Tax Rules

The complexities of international tax legislation, such as the OECD's Base Erosion and Profit Shifting (BEPS) initiatives[395], present developing countries with both obstacles and opportunities. While they aim to reduce tax avoidance tactics that

[388] ILA, Sadowsky, M. e. c. *White Paper 12 on Taxation: Taxing the Future* (International Law Association (2023) <https://www.ilaparis2023.org/en/white-paper/taxation/>, p. 67.

[389] Jemiluyi OO, 'Tax Revenue Mobilization Effort in Southern African Development Community (SADC) Bloc: Does ICT Matter?' (2023), 11(1) *Cogent Economics & Finance*, p. 1.

[390] Bird R and Zolt E, 'Technology and Taxation in Developing Countries: From Hand to Mouse' (2008) *National Tax Journal* 61, p. 42.

[391] Vázquez-Caro J and Bird R, 'Benchmarking Tax Administrations in Developing Countries: A Systemic Approach' (2010) 9 *E Journal of Tax Research*, p. 30.

[392] Addis Tax Initiative, 'The Digital Transformation of Tax Administrations' (*ati*, 19 July 2023) <https://www.addistaxinitiative.net/news/digital-transformation-tax-administrations-0>.

[393] Alm J, 'Tax Evasion, Technology, and Inequality' (2021) 22(4) *Economics of Governance* 321.

[394] 'The Digital Transformation of Tax Administrations';
Alm J, 'Tax Evasion, Technology, and Inequality' (2021) 22(4) *Economics of Governance* 321.

[395] OECD, 'International Collaboration to end Tax Avoidance' <https://www.oecd.org/tax/beps/> accessed 3 October 2023.

disproportionately affect certain countries, implementing the recommended adjustments may be challenging due to these countries' limited resources.[396] Relations between tax administrations of most countries tend to become more multilateral, thanks to common standards and resources such as the Common Reporting Standard (CRS) and other instruments.[397] This requires additional support for the developing countries.

3.2 Exchange of Information (EOI)

From the standpoint of international law, information exchange in tax affairs has become a cornerstone of worldwide efforts to improve transparency and combat tax evasion. A structure of bilateral and international agreements, including Double Taxation Agreements and Tax Information Exchange Agreements, governs this practice[398]. These treaties are reinforced by global standards established by organizations such as the OECD[399] and the UN[400].

The OECD's introduction of the Common Reporting Standard (CRS), which mandates the automated transmission of financial account information between participating nations, has been a significant development in this area. This global program intends to combat cross-border tax evasion by giving tax authorities access to financial data on their inhabitants' assets and income held in other jurisdictions.[401] Effective involvement necessitates significant administrative ability and technology infrastructure.

Furthermore, developed countries may benefit more from international information exchange due to their advanced technology and software, potentially resulting in higher revenue gains. Developing countries may not always have the administrative capacity and knowledge to deal with tax audits arising from the exchange of information that may involve complex transfer pricing issues or complex aggressive tax schemes.[402] Concerns have been also raised regarding these countries' readiness to fulfill the compliance expenses and technical requirements. Questions of data privacy and the need to reconcile taxpayer rights with enforcement objectives add another layer of complication, particularly in areas with weaker data protection regulatory frameworks.

Yet, influencial stakeholders such as Masatsugu Asakawa, President of the Asian Development Bank (ADB), has emphasized the importance of tax transparency and the EOI standards. Asakawa advocates for the effective implementation of these measures across region, highlighting their significance as tools in combating fiscal malpractices.[403]

---

396 ILA, Sadowsky, p. 54.

397 Ibid., p. 91.

398 Individual treaties are available online in the United Nations Treaty Collection, https://treaties.un.org/.

399 OECD, *Exchange of Information*. <https://www.oecd.org/ctp/exchange-of-tax-information/>.

400 UN, *Exchange of Information.* <https://www.un.org/esa/ffd/tax-committee/ta-exchange-information.html>.

401 OECD, *Automatic Exchange Portal. Common Reporting Standard*. <https://www.oecd.org/tax/automatic-exchange/common-reporting-standard/>.

402 Valderrama IJM, 'Legitimacy and the Making of International Tax Law: The Challenges of Multilateralism' (2015) 7(3) *World Tax Journal* 344.

403 Asia Initiative, 'Tax Transparency in Asia 2023: Asia Initiative Progress Report', (2023), <https://www.oecd.org/tax/transparency/documents/tax-transparency-in-asia-2023.htm?utm_campaign=Tax%20News%20Alert%2027-04-23&utm_content=Access%20the%20report&utm_term=ctp&utm_medium=email&utm_source=Adestra>, p. 49.

3.3 International Bodies

On the international level, multilateral organizations like the UN, OECD, World Bank and the International Monetary Fund support tax cooperation in developing countries. The UN Tax Committee, as a subsidiary body of the Economic and Social Council, plays a key role in working with developing countries. Among the most prominent regional organisations are African Tax Administration Forum (ATAF), Asian Development Bank (ADB), Intra-European Organisation of Tax Administrations (IOTA), or Inter-American Center of Tax Administrations (CIAT). These entities often facilitate dialogue, provide platforms for collaboration, and offer technical assistance to harmonize tax systems with international standards. Valderram

In developing countries there is a risk that the gap between advanced economies and lower capacity economies could widen.[404] It is important to recognize and address technological, resource, and people gaps. This recognition is critical for ensuring equitable gains and shared costs from information exchange, as well as enabling all countries to effectively adopt international standards.[405] Experts and aid agencies can help developing countries meet their tax difficulties effectively by assisting in the development of critical human and institutional capacity.[406]

3.4 Examples of International Support and Collaboration

Common, collaborative, digitally enabled and more real time approaches to the administration of common rules is becoming a central feature in the design of international tax rules.[407] The following section will offer several examples of international instruments, forums, and projects of technical assistance in tax matters.

Sustainable Development Goals (SDGs)

Goal 17 of the United Nations Sustainable Development Goals focuses on boosting implementation and reviving the global partnership for sustainable development.[408] Its application also includes investment in technologies and capacity

[404] OECD, 2023 Progress Report on Tax Co-operation for the 21st Century. *OECD Report for the G7 Finance Ministers and Central Bank Governors* (2023) <https://doi.org/doi:https://doi.org/10.1787/d29d0872-en>, p. 29.

[405] Valderrama IJM, 'Legitimacy and the Making of International Tax Law: The Challenges of Multilateralism' (2015) 7(3) *World Tax Journal* 344.

[406] Bird R and Zolt E, 'Technology and Taxation in Developing Countries: From Hand to Mouse' (2008) 61 *National Tax Journal* 791.

[407] OECD, 2023 Progress Report on Tax Co-operation for the 21st Century. *OECD Report for the G7 Finance Ministers and Central Bank Governors* (2023) <https://doi.org/doi:https://doi.org/10.1787/d29d0872-en>, p. 25.

[408] UN, Department of Economic and Social Affairs, *Strengthen the Means of Implementation and Revitalize the Global Partnership for Sustainable Development.* <https://sdgs.un.org/goals/goal17>.

building for tax officials. Given the breadth of issues, capacity building will need to be multi-faceted to ensure long-term outcomes that can help meet the SDGs.[409]

OECD Forum for Tax Administration

The OECD Forum for Tax Administration allows tax administrations from different countries to discuss a group operating in multiple countries to decide how to proceed. This makes it easier to resolve disputes, encourage amicable solutions in the absence of unified tax standards, and gather information on foreign nationals' businesses and activities to boost state tax income.[410] It also offers capacity building, including training, peer-to-peer support, knowledge sharing networks.[411]

Tax Administration Diagnostic Assessment Tool (TADAT)

TADAT launched in 2015 and developed by a consortium of countries and international organizations, is a tool designed to help tax administrations objectively assess their strengths and weaknesses against a baseline of international best practices. The tool has been utilized by 90 tax administrations between November 2013 and February 2020.[412] Although each digitization journey is unique, the agencies can analyze and map regional characteristics. This insight is reflecting regional difficulties, providing regionally specialized recommendations and networking opportunities.[413]

Tax Inspectors Without Borders

Tax Inspectors Without Borders (TIWB) is a joint initiative of the OECD and the United Nations Development Programme (UNDP) supporting countries in building tax audit capacity. Tax experts are sent to developing countries by TIWB. These professionals assist local tax officers in auditing multinational corporations and wealthy individuals. Local tax inspectors learn from real audit cases in this hands-on curriculum. This method develops local tax administration skills and expertise. The current webpage lists running programs.[414]

4. Development and Protection of Taxpayers

4.1 Data Protection and Privacy Concerns in Taxation

Policymakers face new risks for the security of the data that will be used to establish the tax base, subsequently leading to undermining trust regarding use of this data among taxpayers.[415] Furthermore, information technology is not immune to interference or

[409] OECD, 2023 Progress Report on Tax Co-operation for the 21st Century. *OECD Report for the G7 Finance Ministers and Central Bank Governors* (2023) <https://doi.org/doi:https://doi.org/10.1787/d29d0872-en>, p. 29.

[410] ILA, Sadowsky, M. e. c. *White Paper 12 on Taxation: Taxing the Future* (International Law Association (2023) <https://www.ilaparis2023.org/en/white-paper/taxation/>, p. 53.

[411] OECD, *Forum on Tax Administration* <https://www.oecd.org/tax/forum-on-tax-administration/>.

[412] OECD, 'Supporting the Digitalisation of Developing Country Tax Administrations' (2021), p. 132.

[413] Ibid., p. 121.

[414] Tax Inspectors Without Borders. accessible at <http://www.tiwb.org>.

[415] ILA, Sadowsky, p. 68.

systemic corruption prevalent in many developing countries and it may be internally compromised.[416] Technology-based reforms in tax administration must be backed by a functional, modern legal system to realize the full revenue gains and ensure a fair and equitable tax system.[417] To provide a specific example of how such issues are addressed, information security management is a key area of work for many developing countries as they venture into new areas of tax co-operation, notably automatic exchange of information for tax purposes.

Specifically, the Global Forum on Transparency and Exchange of Information for Tax Purposes is an initiative that provides technical assistance to help countries implement and take advantage of information exchange standards. From its modest beginnings, the capacity-building programme has gradually grown to become one of the core activities of the Global Forum Secretariat.[418] Recently, Thailand demonstrated a strong commitment to meeting international standards on transparency and exchange of information (EOI) to combat tax evasion, beginning with its induction program in 2017 and leading to its commitment to the Automatic Exchange of Information standard in 2020 and signing of the CRS-MCAA[419] in 2022. With support from the Global Forum and the Asian Development Bank (ADB), Thailand undertook extensive capacity-building initiatives from 2018 to 2022. Significant strides included adopting enhanced security policies, risk management frameworks, data policies for endpoints and removable devices, and improvements in physical and technological infrastructure. Consequently, Thailand successfully passed its pre-exchange confidentiality assessment. In 2022, 21 detailed technical-assistance reports were produced and provided to Asian members.[420]

4.2 Taxpayer Rights and Access to Technology

Taxpayers' rights must be adapted to new technology contexts as the economy digitizes. This shift in tax collection technologies underlines the absence of proper legal frameworks, posing threats to privacy, defense rights, home security, and legal certainty.[421] Secure data access for corrections, specialized training for tax authorities and institutions, strong data storage and transmission, and complete data security rules are all required to reduce threats to taxpayers. Furthermore, in an era where technology can automate most processes, it seems crucial to retain human oversight for final validation

---

[416] Umar MA and Masud A, 'Why Information Technology is Constrained in Tackling Tax Noncompliance in Developing Countries' (2020) 33(2) *Accounting Research Journal* 307.

[417] Okunogbe O and Santoro F, 'The Promise and Limitations of Information Technology for Tax Mobilization' (2023) 38(2) *The World Bank Research Observer* 295.

[418] OECD, '10 Years of Capacity Building. 2022 Global Forum Capacity Building Report' (2022), <https://www.oecd.org/tax/transparency/documents/2022-Global-Forum-Capacity-Building-Report.pdf >.

[419] The CRS MCAA specifies the details of what information will be exchanged and when.

[420] Asia Initiative, 'Tax Transparency in Asia 2023: Asia Initiative Progress Report', (2023), <https://www.oecd.org/tax/transparency/documents/tax-transparency-in-asia-2023.htm?utm_campaign=Tax%20News%20Alert%2027-04-23&utm_content=Access%20the%20report&utm_term=ctp&utm_medium=email&utm_source=Adestra>, p. 40.

[421] ILA, Sadowsky, p. 112.

and interpretation. Tax officials must be equipped with specialized computer training to manage potential system failures.[422]

A perception of the taxpayers also remains of importance. A study conducted in Pakistan confirms a strong association between fairness perception and tax compliance, aligning with existing literature that suggests taxpayers are more likely to evade taxes if they view the tax system as unfair. [423] Taxpayers may be also hesitant to use technology tools due to lack of information and trust, security concerns, or high costs of adoption.[424] The current Annual Report of the IBFD Observatory for the Protection of Taxpayers' Rights included an observation that increased use of digital resources could present challenges, particularly for those members of society who may not have access to or be familiar with technology and may struggle to navigate the digital landscape.[425]

In many low- and middle-income nations, infrastructural shortages, such as restricted internet and energy access, might inhibit taxpayers' effective adoption of technology, particularly among the disadvantaged, raising issues about equity.[426] Businesses, particularly small and medium-sized firms (SMEs), require IT infrastructure to comply with tax administration. Unfortunately, a huge portion of developing-country SMEs do not yet have access to basic IT infrastructure.[427] Based on the outcomes of the study conducted in Southern African Development Community, affordability of ICT products should be prioritized to give wider access to internet usage in order to eradicate the challenge of digital divide.[428] For example, a recent study using data from Ethiopia evaluated the impact of Electronic Sales Register Machines (ESRMs) on tax collection. It found that even though VAT collections increased following ESRM adoption, there was a slight negative impact on new firm entry, hinting at a potential reduction in the tax base.[429] This could suggest a technological barrier. Even developing countries may consider supplying or subsidizing tax planning and preparation software for low-income population.[430]

Conclusion

The purpose of this article was to offer a more complex view of opportunities and problems of tax and technology in developing countries, including a variety of practical examples and studies. As proven by successful projects such as Rwanda's Electronic

422 Ibid., pp. 109, 112–113.

423 Perveen N and Ahmad A, 'Tax Technology, Fairness Perception and Tax Compliance among Individual Taxpayers' (2023) 2(2) *Audit and Accounting Review* 99, p. 113.

424 Okunogbe O and Santoro F, 'The Promise and Limitations of Information Technology for Tax Mobilization' (2023) 38(2) *The World Bank Research Observer* 295, p. 318.

425 Baker P, Pistone P and Turina A, 'The IBFD Yearbook on Taxpayers' Rights 2022' (*IBFD*, 15 May 2023) <https://www.ibfd.org/sites/default/files/2023-05/optr-yearbook-2022_for-release-120523.pdf>, p. 41.

426 'The Promise and Limitations of Information Technology for Tax Mobilization', p. 318.

427 Umar MA and Masud A, 'Why Information Technology is Constrained in Tackling Tax Noncompliance in Developing Countries' (2020) 33(2) *Accounting Research Journal* 307, p. 307.

428 Jemiluyi OO, 'Tax Revenue Mobilization Effort in Southern African Development Community (SADC) Bloc: Does ICT Matter?' (2023) 11(1)*Cogent Economics & Finance* 1, p. 10.

429 Ali M, Shifa AB, Shimeles A and Woldeyes F, 'Building Fiscal Capacity in Developing Countries: Evidence on the Role of Information Technology' (2021) 74(3) *National Tax Journal* 591, pp. 616–617.

430 Walker DI, 'Tax Complexity and Technology' (2022) 97(4) *Indiana Law Journal* 1095, pp. 1142–1143.

Billing Machines and Nigeria's TaxPro-Max platform, technological improvements have significant promise for improving tax compliance and increasing the tax base. These tools have been shown to be successful in reducing concerns such as tax evasion and poor record-keeping while also streamlining compliance processes for taxpayers. The digital transformation of tax administration, on the other hand, is not without complexities. The challenges for developing countries include assuring proper data protection and privacy or maintaining legal certainty. It also emphasizes the importance of protecting taxpayers' rights in an increasingly digital society. While technology can improve efficiency and expedite operations, it also raises concerns about fairness, access, and equity. For example, in low and middle-income nations, infrastructure deficiencies such as insufficient internet and energy access can hinder effective technology adoption, particularly among disadvantaged population. It is also important to emphasise the significance of international cooperation and capacity building. Initiatives such as the Global Forum's capacity-building program and the Tax Inspectors Without Borders project are critical in assisting developing countries in meeting international transparency and information-sharing criteria.

In the future, the area of technology and taxation will bring many new challenges and questions. How will emerging technologies such as blockchain and AI continue to transform tax systems? What policies and structures are required to ensure that the advantages of digitalization are distributed equally and that all taxpayers' rights are protected? And, perhaps most crucially, how can developing countries effectively address these shifts while dealing with their own particular issues and resource constraints? As we progress, the necessity for continued research, policy innovation, and international collaboration becomes increasingly important in ensuring that global tax system digitization is equitable, efficient, and respectful of taxpayer rights.

4.2 Bridging the Gap: A Legal Analysis of Artificial Intelligence's (AI) Impact on Promoting the Right to Health in Developing Countries

By ***Oshokha Caleb Ilegogie*** (Charles University)

Introduction

The right to health has been aptly described as a right that one would need help finding a more controversial or nebulous human right.[431] This right is characterized as a ubiquitous right whose actual meaning appears elusive despite its meaning being commonly assumed to be understood by all, mainly due to its status as a recognized human right under international law.[432] This misunderstanding of what the right to health entails can be attributed to conceptual confusion, as well as a lack of effective implementation of the right, which provides a source of significant problems for policymakers seeking to deploy the right to health as a strategy to influence health outcomes and implement their obligations under international law. The lack of a clear universal definition of the right is also confusing. It creates structural problems within international law, placing significant constraints on understanding what the right means, even for those working in the health and human rights field.[433]

The right to health stems primarily, although not exclusively, from Article 12 of the International Covenant on Economic, Social, and Cultural Rights (ICESCR) and requires State governments to recognize "the right of everyone to the highest attainable standard of physical and mental health."[434] However, to avoid going into further detail,

[431] Ruger JP, 'Toward a Theory of a Right to Health: Capability and Incompletely Theorized Agreements' (2006) 18(2) *Yale J Law Humanit* 273, p. 3.

[432] Ibid.

[433] Lawrence G, 'Global Health Law Governance' (2008) 22 *Emory International Law Review* 35, pp. 35–36.

[434] The right to healthcare was first articulated in the WHO Constitution (1946) which states that: „the enjoyment of the highest attainable standard of health is one of the fundamental rights of every human being…". The preamble of the Constitution defines health as: "A state of complete physical, mental and social well-being and not merely the absence of disease or infirmity". The 1948 Universal declaration of Human Rights mentioned health as part of the right to an adequate standard of living (article 25). It was again recognised as a human right in 1966 in the International Covenant on Economic, Social and Cultural Rights, Article 12 which states: "1. The States Parties to the present Covenant recognise the right of everyone to the enjoyment of the highest attainable standard of physical and mental health. 2. The steps to be taken by the States Parties to the present Covenant to achieve the full realisation of this right shall include those necessary for: (a) The provision for the reduction of the stillbirth-rate and of infant mortality and for the healthy development of the child; (b) The improvement of all aspects of environmental and industrial hygiene; (c) The prevention, treatment and control of epidemic, endemic, occupational and other diseases; (d) The creation of conditions which would assure to all medical service and medical attention in the event of sickness." This right can also be found in regional human rights instruments, which include: American Declaration on the Rights and Duties of Man (art. 33), European Social Charter (art. 11) and African Charter on Human and Peoples' Rights (art. 16). The right to

this paper does not mainly focus on the concept of the right to health. In an attempt to prevent further perpetuation of the existing conceptual confusion regarding the right to health, this paper embraces the simplified understanding of the right to health as "the right of every individual to access the necessary determinants of health, required to enjoy the highest attainable standard of physical and mental health."[435] Understanding the right in this light is predicated on protecting and promoting human dignity, the central tenet of the right to health.

The effective promotion of the right to health and access to healthcare is, however, subject to the availability of resources of subjective state governments, with resource constraints typically being the primary determinant that prevents the successful implementation of the duty of state governments to promote this right.[436] These resource constraints, mainly financial and human resource constraints are especially felt in developing nations, as individuals in less developed countries tend to have less access to healthcare services compared to their contemporaries in developed countries. This paper categorizes developing countries as countries whose governments typically fail to meet their obligations that promote and protect the right to health under international law, and sometimes under domestic constitutional law, by allocating little to no resources to healthcare and having deficient healthcare standards. These countries typically rely heavily on the private and international sectors for the provision of healthcare, as the governments in these countries usually fail to meet the minimum level of government involvement that is necessary to meet basic healthcare needs, causing the standard of healthcare of the populations of these nations to suffer.

Although the problem of access to healthcare services is also reflected within countries (regardless of their stage of development), as poorer members of society tend to have less access to health services compared to their wealthier contemporaries.[437] Lack of financial resources can create barriers to accessing health services, as the causal relationship between access to health services and poverty runs contemporaneously, with limited access to healthcare worsening the health outcomes of individuals, resulting in loss of income and higher healthcare costs, both of which contribute to poverty and negatively affect the development of a nation.[438] Deprivation of access to healthcare creates poorer, undeveloped nations and puts societies at risk, as poverty leads to ill health, and ill health maintains poverty, which stagnates national development.

Considering the preceding, this paper seeks to contribute to the discussion on the benefits and ethical and legal implications of adopting an emerging technological advancement like Artificial Intelligence (AI) to sustainably promote the right to health in developing countries. This paper avers that despite the potential of AI as a tool to

healthcare is relevant to all States: every State has ratified at least one international human rights treaty that recognises the right to healthcare.

435 Chapman A, 'The Foundations of a Human Right to Healthcare: Human Rights and Bioethics in Dialogue, Health and Human Rights' (*HHR*, 9 June 2015).

436 Article 2 ICESCR.

437 Peters DH et al, 'Poverty and Access to Health Care in Developing Countries' (2008) 1136 *Annals of the New York Academy of Sciences* 161.

438 Guo J and Li B, 'The Application of Medical Artificial Intelligence Technology in Rural Areas of Developing Countries' (2018) 2 *Health Equity* 174.

accelerate access to healthcare, real concerns must be addressed, bordering on issues relating to transparency, data ownership and privacy, and patient safety, amongst other topics. This paper, therefore, presents an ethical and legal analytical view of the application of AI in promoting access to healthcare in nations categorized as developing countries and shall focus mainly on Nigeria, the African continent's most populous nation, with a population exceeding 200 million individuals.[439] The Nation's Human Capital Index raises concerns, as it ranks among the bottom 24 countries out of 174 worldwide, with a score below 0.4, underscoring the urgent need to address the nation's ailing healthcare sector to harness the potential of the country's demographic dividend fully and to guarantee the nation's future prosperity and sustainable growth.[440]

Hence, this paper seeks to answer the research questions: 'What are the legal implications of implementing AI to promote the right to health and access to healthcare for developing countries' and 'How can legal, regulatory reform address the ethical and legal implications of adopting AI to solving access to healthcare issues in these developing countries?' To answer these questions, this paper recognizes that the promotion of the right to health is a global concern that is particularly urgent in the least developed countries of the world today because, by their very nature and categorization, they are the least developed and lack the necessary financial and human resources required to promote access to healthcare. Thus, the proper application of AI to this issue provides a sustainable alternative solution for providing effective resource management, accurate diagnosis, and prediction of various critical health issues, with the successful implementation of this technology having the potential to bring immense benefits to individuals in these developing nations. Pursuing a solution to the problem of access to healthcare and resource constraints in developing countries makes Nigeria an excellent case study to explore the questions posed by this paper. It presents an opportunity to examine the benefits of adopting AI to address this problem.

1. The impact of AI on the right to health

In simple terms, AI is the process through which a computer system mimics human intellectual functions, such as the ability to reason, make decisions, generalize, or learn from prior experience to accomplish objectives without being explicitly programmed for particular actions.[441] AI also involves processes such as adaptation, sensory understanding, and interaction, which, in comparison to traditional computational algorithms (which are software programs that follow a set of rules and consistently do the same task), an AI system, on the other hand, learns the rules (function) through training data (input) exposure to give results. [442] Due to this distinction, AI has the

[439] UN, Department of Economic and Social Affairs Population Division, *World Population Prospects 2019, vol II. Nigeria: Demographic Profiles*, <https://population.un.org/wpp/publications/files/wpp2019_highlights.pdf>.

[440] World Bank, 'The Human Capital Index 2020 update: human capital in the time of COVID-19', (2020) <https://openknowledge.worldbank. org/handle/10986/34432>.

[441] McCarthy J, Minsky ML, Rochester N, Shannon CE, 'A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence, August 31, 1955' (2006) 27(4) *AI Magazine* 12.

[442] Drukker L, Noble JA, Papageorghiou AT, 'Introduction to artificial intelligence in ultrasound imaging in Obstetrics and Gynecology' (2020) 56 *Ultrasound Obstetr Gynecol* 498.

potential to impact healthcare by producing new and essential insights from the vast amount of digital data created during healthcare delivery to deliver novel solutions.[443]

AI refers to machines' intelligence and includes machine learning, natural language processing, and robotics, with a wide application in healthcare, possessing the potential to contribute to biomedical research, medical education, and healthcare delivery.[444] Some AI experts have proposed that something 'acts intelligently' when it does what is appropriate for its circumstances and purposes, is flexible to changing environments and goals, learns from experience, and makes the right choices given its perceptual and computational limitations.[445] Learnability comprises the critical feature of AI, and machine learning (ML), the dominant approach in AI, is responsible for most of the recent technological advancements in the field. Machine learning typically refers to a system that trains a predictive model by identifying data patterns from input and then uses such a model to make useful predictions from new, never-before-seen data.[446] AI algorithms also use supervised and unsupervised machine learning techniques for autonomous decision-making, as these machine learning algorithms automatically learn and improve themselves from experience without being explicitly programmed, resulting in their application to many data types (including images, speech, videos, and text) on complex tasks that involve large amounts of data to produce results that are comparable to and sometimes superior to human experts in terms of both accuracy and efficiency.[447] This ability to analyze large amounts of data and learn independently depicts the potential benefits of AI implementation in promoting the right to health of individuals and increasing access to healthcare by enhancing the proficiency of clinical work, preventing medical errors, and providing data-driven, evidence-based clinical decisions for advancing medical diagnosis, treatment decisions, biomedical research, and service delivery across the full spectrum of healthcare.[448]

In healthcare settings, incorporating AI technology can benefit administrative and clinical processes, including patient safety, hospital administration, drug research, and production, and assist healthcare professionals in making expedient and reliable treatment decisions relying exclusively on data.[449] The technological advancements of AI have also improved other aspects of healthcare delivery, especially in the areas of diagnosis and treatment, by enabling real-time patient information to be easily accessible for physicians, paving the way for fast care management in specific scenarios,

[443] Sousa WG et al, 'How and Where Is Artificial Intelligence in the Public Sector Going? A Literature Review and Research Agenda' (2019) 36 *Government Information Quarterly* 101392.

[444] Ramesh A et al, 'Artificial Intelligence in Medicine' (2004) 86 *Annals of The Royal College of Surgeons of England* 334.

[445] Poole DL, Mackworth AK, *Artificial Intelligence: Foundations of Computational Agents* (CUP, 2010).

[446] Ali S et al, 'Explainable Artificial Intelligence (XAI): What We Know and What Is Left to Attain Trustworthy Artificial Intelligence' (2023) 99 *Information Fusion* 101805.

[447] Kalmady SV et al, 'Towards Artificial Intelligence in Mental Health by Improving Schizophrenia Prediction with Multiple Brain Parcellation Ensemble-Learning' (2019) 5(1) *Schizophrenia* 2.

[448] Osop H, Sahama T, 'Data-Driven and Practice-Based Evidence: Design and Development of Efficient and Effective Clinical Decision Support System' in Moon JD, *Improving Health Management through Clinical Decision Support Systems* (IGI Global, 2016).

[449] Madsen LB, *Data-Driven Healthcare: How Analytics and BI Are Transforming the Industry* (Wiley, 2014).

especially in emergencies and in situations where immediate medical intervention is required to reduce casualties.[450] This technological advancement also improves existing healthcare systems, specifically in medical imaging and coronary artery disease diagnosis, by reducing human error, increasing patient care, and reducing the workload on healthcare professionals, which are currently reported as insufficient for the growing global populace.[451] In Nigeria, it is estimated that the ratio of medical doctors per 10,000 citizens currently stands at 3.95, as there are currently only 84,277 medical doctors, marking a considerable human resource shortage in comparison to the World Health Organization's (WHO) recommended ratio of 1 doctor to 600 individuals.[452] It is also reported that this figure is possibly an overestimation, as it only considers the total number of medical doctors registered in Nigeria but does not consider those who might have died, retired, changed professions, or emigrated from the country.[453] Nigeria is reported to be the country with the highest medical workforce export in Africa to destinations including the United Kingdom, Canada, United States, Australia, and Saudi Arabia.[454] The scale of this mass emigration is depicted in a national statistical report published in 2022 by the UK government, which revealed that 13,609 healthcare workers left Nigeria for the UK between 2021 and 2022.[455] This number is speculated to keep rising, reducing the number of healthcare professionals available to administer proper healthcare services, thus inhibiting proper access to healthcare services.

In such a dire setting as is reflected in Nigeria, AI has the potential to bridge the human resource constraints, as AI algorithms applied in medical diagnosis typically match the professional expert level of healthcare practitioners and, in some cases, even surpass experts in diagnosing malignant tumors.[456] AI is also currently applied in drug discovery to guide researchers in assembling groups of participants for costly clinical trials.[457] As developing countries like Nigeria currently struggle with a high burden of disease, lack of trained healthcare providers, and poor healthcare delivery infrastructure, it is in these settings that AI has a tremendous potential to promote access to healthcare by reducing costs incurred due to accessing healthcare services, reducing health inequity

---

[450] Bini SA, 'Artificial Intelligence, Machine Learning, Deep Learning, and Cognitive Computing: What Do These Terms Mean and How Will They Impact Health Care?' (2018) 33 *J. Arthroplast* 2358.

[451] World Health Organization, 'World health statistics 2023: Monitoring health for the SDGs, Sustainable Development Goals,' (2023) <https://www.who.int/publications/i/item/9789240074323>.

[452] World Health Organization, 'Health workforce: medical doctors' <https://www.who.int/data/gho/data/themes/topics/health-workforce>.

[453] Onah CK and others, 'Physician Emigration from Nigeria and the Associated Factors: The Implications to Safeguarding the Nigeria Health System' (2022) 20 *Human Resources for Health* 80.

[454] Emigration of Nigerian Medical Doctors Survey Report 2018. NOI Polls, Abuja <https://noi-polls.com/emigration-of-medical-doctors-still-a-major-issue-in-nigeria/> accessed 4 December 2023.

[455] 'National statistics: Why do people come to the UK? To work' (*London: Gov.UK*, 2022) <https://www.gov.uk/government/statistics/immigration-statistics-year-ending-march-2021/why-do-people-come-to-the-uk-for-family-reasons>.

[456] Hunter B, Hindocha S, Lee RW, 'The role of artificial intelligence in early cancer diagnosis' (2022) 14(6) *Cancers* 1524.

[457] He J et al, 'The Practical Implementation of Artificial Intelligence Technologies in Medicine' (2019) 25 *Nature Medicine*.

through early disease detection and diagnosis, and improving the efficiency and quality of existing healthcare services.[458]

Developed countries are reportedly already benefiting from integrating AI into their healthcare ecosystems, with an analysis projecting that approximately $150 billion will be saved in healthcare costs annually by 2026 in the USA.[459] The existing integration of AI into healthcare delivery in developed countries raises optimism of AI integration into the healthcare delivery of developing countries, as it could also prove transformative for public health in these countries, especially considering the successful adoption rate of previous technological advancements, including mobile phone penetration, developments in cloud computing and substantial investments in digitizing health information and introducing mobile health applications in these countries. As a result, these developing nations now have the necessary data and basic infrastructure to initiate meaningful use of AI applications. Advances in AI could also help expand and strengthen the impact of these and other digital health technologies in these nations.[460] The potential impact of AI, particularly ML, to significantly contribute to healthcare reform in developing countries is significant if properly utilized to address the issues of increasing patient demand, chronic diseases, and resource constraints, which continue to pressure the healthcare systems. This mandates the proper implementation of AI so that healthcare practitioners in these nations can focus more on the causes of ill health and keep track of successful preventative methods and interventions.[461]

The advantages of applying AI to healthcare delivery in developing nations can be seen in countries like Egypt, where a medical AI tool was applied to detect common eye disorders and was used as far back as the 1980s.[462] Another example of AI use in developing nations is seen in the example of a Nigerian startup that applies medical AI tools to address access to healthcare issues by using signal processing and machine learning to improve the diagnosis of birth asphyxia in low-resource settings.[463] From the preceding, the emerging technological advancements of AI and its benefits to healthcare delivery are auspicious, as it has the potential to address several issues currently plaguing the current healthcare landscape, particularly in addressing the significant access to healthcare disparities existing between the global population, as well as within urban and rural populations. With the prevalence of issues such as the scarcity of qualified healthcare professionals, which significantly contributes to the limited access and subpar quality of healthcare services, the application of AI to healthcare delivery can eradicate these problems and minimize these challenges.

---

458 Ibid., (Fn 7).

459 Bohr A, Memarzadeh K, 'The rise of artificial intelligence in healthcare applications' (2020) 12(3) *Artificial Intelligence in Healthcare* 25.

460 Stoumpos AI, Kitsios F, Talias MA, 'Digital Transformation in Healthcare: Technology Acceptance and Its Applications' (2023) 20 *International Journal of Environmental Research and Public Health* 3407.

461 Naik N et al, 'Legal and Ethical Consideration in Artificial Intelligence in Healthcare: Who Takes Responsibility?' (2022) 9 *Frontiers in Surgery* 1.

462 Kastner JK et al, 'An Expert Consultation System for Frontline Health Workers in Primary Eye Care' (1984) 8 *Journal of Medical Systems* 389.

463 Owoyemi A et al, 'Artificial Intelligence for Healthcare in Africa' (2020) 2 *Frontiers in Digital Health* 1.

Following this examination of the potential to promote the right to health through the adoption of AI, on the one hand, AI holds the promise of being a catalyst in accelerating access to healthcare and allowing developing nations to leapfrog over some traditional obstacles that affect access to healthcare. However, on the other hand, this adoption of AI brings along challenges that exist in the form of technological, ethical, and legal challenges, which must be addressed to ensure proper promotion of the right to health rather than perpetuating further harm by limiting access to health for specific individuals. Addressing these issues is vital because the application of AI in public health systems, particularly to data gathering, diagnosis, and interpretation of medical data, raises significant concerns, mainly due to the sensitive and confidential nature of healthcare delivery. This especially borders on issues of trust and reliability, which become prominent as AI-driven healthcare systems carry sensitive health information and high-end patient vulnerabilities.[464] The subsequent sections of this paper shall address these issues in detail and postulate solutions for creating strong and effective legal and regulatory frameworks, which will guarantee a proper implementation of AI systems to address access to healthcare issues in the public healthcare sector of developing nations.

2. Challenges encountered applying AI to right to health issues

Patient safety

Patient safety is a primary challenge when discussing AI's application to solving access to health issues today. The black-box design of most AI systems (which means that these AI algorithms typically fail to explain why a given input data produces a corresponding output) makes it challenging to provide a reason for the AI system's decisions or to portray its findings logically or reasonably.[465] This issue mandates AI algorithms to be transparent, interpretable, and explainable to retain human agency and patient autonomy concerning treatment decisions, which is especially important for promoting the right to health and access to healthcare because the right to health is based on principles of safeguarding human dignity and promoting the well-being of people.[466] These principles are vital and recognized in several policy guidelines on AI development and relate to a critical implication when balancing ethical implications of patient safety and autonomy.[467]

The black-box model of AI systems creates a problem for healthcare practitioners who apply AI to patient care and makes it impossible to inspect the decision-making process of the AI system, leading to a lack of understanding of the AI's decisions.[468] This

[464] Joshi S et al, 'Modeling Conceptual Framework for Implementing Barriers of AI in Public Healthcare for Improving Operational Excellence: Experiences from Developing Countries' (2022) 14 *Sustainability* 11698.

[465] Tonekaboni S, Joshi S, McCradden MD, Goldenberg A, 'What clinicians want: Contextualizing explainable machine learning for clinical end use' (2019) 1 *Proceedings of Machine Learning Research* 21.

[466] Floridi L and Cowls J, 'A Unified Framework of Five Principles for AI in Society' (2019) 1(1) *Harvard Data Science Review* 1.

[467] Gregory A and Halff G, 'The Damage Done by Big Data-Driven Public Relations' (2020) 46 *Public Relations Review* 101902.

[468] Kim H and Xie B, 'Health Literacy in the eHealth Era: A Systematic Review of the Literature' (2017) 100 *Patient Education and Counseling* 1073.

black-box model further results in difficulties in revealing the accuracy of the decision-making mechanism of the AI algorithm and prohibits healthcare professionals from being able to disclose the inner workings of the AI model.[469] The black-box model also prevents users of AI systems, including physicians and patients, from having little opportunity to interrogate and challenge the operation of AI algorithms and their outcomes, thus making it difficult to guarantee a transparent decision-making process that is explainable, allowing for informed consent by patients, thereby affecting their ability to choose or refuse certain treatment decisions.[470] The black-box model also prevents the decisions of AI algorithms from being audited by competent authorities and makes harm untraceable in situations in which they occur.[471]

The ability to Interpret and explain the decisions of an AI algorithm enables those applying AI to healthcare services to delve into the decision-making process to promote confidence in understanding where the AI model gets its results and increases patient safety by giving additional information that is essential for interpreting an AI algorithm's underlying functioning. This ability to explain the decision-making process of the AI provides insights into the AI's decision to the healthcare operators to build trust that the AI algorithm is making correct and non-biased decisions based on the facts pertinent to the treatment of the patient to which the AI system is applied to and ensures that the AI algorithm is making correct and non-biased decisions based on the facts before it. Explainability is vital to decision-making about treatments and disease prevention, particularly in cases relating to specific patients, as patients must understand that their treatment decisions are meaningfully made.[472]

When this decision-making process in an AI system is thoroughly understood, the AI system becomes transparent and promotes patient safety and trust in the AI system. Developing countries who wish to take up AI to facilitate access to healthcare issues should encourage transparency in the decision-making process of AI algorithms and can do this by shifting their focus from matters surrounding trust in AI systems to focusing more on promoting the development and application of responsible AI systems, for example, by introducing post-market surveillance and audits of medical care delivery and outcomes.[473] Governments of developing nations should also encourage designing AI systems that consider their local peculiarities, including the multidimensionality of health, such as physical, mental, emotional, social, spiritual, vocational, and other dimensions of health, per the principles of fairness and justice.

---

469 Gunning D et al, 'XAI—Explainable Artificial Intelligence' (2019) 4(37) *Science Robotics* 7120.

470 Ploug T and Holm S, 'The Right to Refuse Diagnostics and Treatment Planning by Artificial Intelligence' (2019) 23 *Medicine, Health Care and Philosophy* 107.

471 Wachter R, *The Digital Doctor: Hope, Hype, and Harm at the Dawn of Medicine's Computer Age* (McGraw-Hill Education, 2017).

472 Wachter S, Mittelstadt B, Floridi L, 'Transparent, Explainable, and Accountable AI for Robotics' (2017) 2(6) *Science Robotics* 6080.

473 La Fors K, Custers B and Keymolen E, 'Reassessing Values for Emerging Big Data Technologies: Integrating Design-Based and Application-Based Approaches' (2019) 21 *Ethics and Information Technology* 209.

Data privacy issues

The amount and types of data generated today in healthcare settings significantly outpace the ability of humans to consume, comprehend, and use to inform non-trivial patient care decisions compared to AI tools, which can process these information and come up with a prompt decision. The AI tools applied in healthcare settings require vast amounts of high-quality data to learn to perform efficiently and to perform their functions properly. However, this reliance on high-quality data creates enormous concerns regarding data privacy.[474] These concerns, especially in healthcare settings, are warranted, where the data required for training AI systems and their successful functioning involves sensitive and confidential patient information. In the event of incidents of data leakage or misuse, there are serious consequences, as it could result in serious harm to patients and healthcare providers since this data predominantly contains sensitive patient information, including confidential conversations between healthcare professionals and their patients, patients' health records, and identity information.[475]

In today's world, the capacity of individuals to manage how personal data is kept, updated, and shared between parties is critical to data privacy. Recently, with the introduction of powerful internet-based data mining tools, data privacy-related issues have become rampant, making data privacy and control over personal information increasingly crucial.[476]

Individuals, while applying AI tools to promote their access to healthcare, have limited oversight over what passive data is collected and how that data is transformed into a recommendation or healthcare decision, limiting their ability to challenge any decisions made and may result in a loss of personal autonomy, as well as raise data privacy issues.[477] The critical components of privacy protection and AI applications to address access to healthcare issues add to the risks to individual privacy. This risk is exacerbated, particularly in developing countries, which are unlike many developed nations that have strong data protection laws that aim to protect the privacy of their citizens, including countries like the United States, which passed the Health Insurance Portability and Accountability Act (HIPAA) in 1996 to strengthen the law to protect healthcare facilities, and the General Data Protection Regulation (GDPR) applicable in the European Union which acts as the data protection and privacy regulation that prescribes stringent rules that must be respected while working with data belonging to individuals.

The risks involved in applying AI tools to address access to healthcare issues in developing nations include pertinent risks that must be prevented by the adoption

---

[474] Davenport T, Kalakota R, 'The Potential for Artificial Intelligence in Healthcare' (2019) 6 *Future Healthcare Journal* 94.

[475] Kitkowska A, Karegar F and Wästlund E, 'Share or Protect: Understanding the Interplay of Trust, Privacy Concerns, and Data Sharing Purposes in Health and Well-Being Apps' (2023) *CHItaly 2023: 15th Biannual Conference of the Italian SIGCHI Chapter*. Copeland BJ, 'Artificial Intelligence', Encyclopaedia Britannica <https://tinyurl.com/mt592fcv> accessed 15 October 2023.

[476] Manheim K and Kaplan L, 'Artificial Intelligence: Risks to Privacy and Democracy' (2019) 21 *Yale JL & Tech* 106.

[477] Kleinpeter E, 'Four Ethical Issues of E-Health' (2017) 38 *IRBM* 245.

of similar stringent data protection regulations to avoid data exploitation, which includes the illegal use of individuals' private data, illegal identification and tracking of individuals due to data breaches. Other risks that developing countries that seek to apply AI tools to address access to healthcare issues must be aware of include risks relating to re-identification and de-anonymization of sensitive medical and personal data. To address these issues successfully, developing countries will need to proactively adopt stringent regulations like the GDPR for example, which introduced strict consent requirements for data collection, giving individuals the right to control their data while strictly regulating parties that collect, control, and process data, with significant fines for failure to comply with the Regulation. Emulating these laws and adopting them to address our local peculiarities will make actors, data controllers, and stakeholders applying AI tools in healthcare settings in these developing nations accountable and responsible.[478]

Developing countries seeking to ensure adequate data protection may also take a page from Nigeria, which recently adopted the Nigeria Data Protection Act (NDPA), 2023, to replace the Nigerian Data Protection Regulations (NDPR) 2019 and the NDPR Implementation Framework 2019, issued under the National Information Technology Development Agency (NITDA) Act. The NDPA establishes the legal framework for regulating personal data in the country and seeks to ensure that personal data protection is a guaranteed fundamental human right, with the aims of safeguarding the fundamental rights and freedoms of data subjects protected under the Nigerian Constitution, regulating the processing of personal data, promoting data processing best practices that ensure the security of personal data and the privacy of data subjects's rights by regulating data collectors and processors, as well as strengthening the legal foundations of the Nigerian digital economy and guaranteeing the Nation's participation in regional and global economies through beneficial and trusted use of personal data.[479]

The NDPA also establishes the Nigeria Data Protection Commission (NDPC), which implements and enforces the rules and regulations set out in the Act and regulates the processing of personal information and other related matters.[480] The Act also establishes a Governing Council of the Commission, which is responsible for formulating and providing overall policy directions for the affairs of the NDPC.[481] The NDPC is responsible for investigating data privacy complaints and can autonomously initiate inquiries when there is suspicion of privacy violations. This mandate upholds transparency and fosters accountability among businesses processing personal data.[482]

The NDPA stipulates penalties for contravention of the Act and or its subsidiary regulations, subject to variation based on the significance of the roles played by the data controllers or data processors involved in the breach, wherein entities engaged in the processing of larger volumes of personal data are held to an elevated data protection standards and increased accountability measures. This approach ensures that entities

[478] Wakunuma K, Jiya T, Aliyu S, 'Socio-Ethical Implications of Using AI in Accelerating SDG3 in Least Developed Countries' (2020) 4 *Journal of Responsible Technology* 100006.

[479] *Data Protection Act*, Nigeria (2023), Section 1.

[480] Ibid., Section 4.

[481] Ibid., Section 8.

[482] Ibid., Section 46.

handling substantial amounts of personal data are subject to commensurate regulatory expectations, aligning with safeguarding individual privacy and data security. According to the NDPA, for data controllers or processors of 'major importance,' the maximum fine for breaching the personal data of individuals is stipulated at being between the greater of ₦10,000,000 (ten million Naira) or 2% of the annual gross revenue of the data controller's preceding financial year, and for less significant data controllers or processors, the maximum fine for data breaches is the more significant sum between ₦2,000,000 (two million Naira) or 2% of their annual gross revenue in the preceding financial year.[483] This marks a significant improvement on the penalties previously outlined in the repealed NDPR 2019, which levied a fine of 2% of the annual gross revenue or ₦10 million (ten million Naira) for breaches involving over 10,000 data subjects and 1% of the annual gross revenue or ₦2 million (two million Naira) for breaches involving fewer than 10,000 data subjects.[484]

Because the law was recently passed, it is anticipated that the NDPC will issue regulations and guidelines to clarify the compliance requirements outlined in the Act. This includes defining the parameters for classifying a data controller or processor as one of 'major importance,' specifying the frequency and content of compliance returns for such entities, and outlining steps for data controllers to inform subjects of personal data breaches adequately.[485]

The enactment of this law by the Nigerian government establishes robust safeguards for data protection. It ensures that integrating AI tools in healthcare settings prevents data privacy breaches. It sets a precedent for developing countries aspiring to institute comprehensive data protection laws, thereby safeguarding data protection as a fundamental human right.

Bias

Issues relating to bias and fairness are predicated on the ethical obligation that mandates that all humans should be treated equally and stipulates that the application of AI should not result in unfair discrimination against individuals, communities, or groups.[486] However, despite AI's potential to address healthcare issues in developing countries and improve health outcomes of individuals living in these disadvantaged nations, the opposite unintended effect of AI tools restricting access to healthcare to individuals may arise due to issues relating to bias. This issue may arise because AI tools perpetuate bias and unfairness due to the training data used in the development stage that reflects existing biases in diagnosis, treatment, and provision of services to marginalized populations or through algorithmic bias.[487] In such a scenario, the AI tool

[483] Ibid., Fn 479, Section 48.

[484] *Data Protection Regulation*, Nigeria (2019)

[485] KPMG, The Nigeria Data Protection Act, 2023 A Review of the Key Compliance Provisions and their Implications for Nigerian Businesses (2023).

[486] Fountain JE, 'The moon, the ghetto and artificial intelligence: Reducing systemic racism in computational algorithms' (2022) 39 *Governmental Information Quarterly* 101645.

[487] Ferryman K, Pitcan M, 'Fairness in precision medicine' (*Data & Society*, February 2018) <https://datasociety.net/wp-content/uploads/2018/02/Data.Society.Fairness.In_.Precision.Medicine.Feb2018.FINAL-2.26.18.pdf>.

risks automating and worsening that bias as it continues to learn through subsequent cycles and continually perpetuates it.[488] Algorithmic bias may also occur which happens when an AI model, trained on a given data set, produces results that may be wholly unintended by the model creators; because AI tools, particularly those applying machine learning, rely on vast amounts of data, such bias can be encoded within the AI's modeling choices or even within the data itself.[489] The AI system then acts unfairly, as it cannot make unbiased decisions without favoring any of the populations represented in the input data distribution.[490]

Ideally, to prevent bias, AI tools have access to exhaustive sources of population electronic health record data to create representative models for diagnosing diseases, predicting adverse effects, and recommending ongoing treatments. However, in developing countries, such comprehensive data sources may only sometimes be available due to various socio-economic issues, typically financial and infrastructure deficits and other technical problems.[491]

Bias may affect the decisions of AI systems in various ways, including relying on biased information such as the gender, location of birth, socio-economic background, and skills of individuals to determine the treatment outcomes for these individuals. The existence of bias in some datasets and algorithms may also result in different access to healthcare outcomes for groups of individuals, resulting in unfair treatment and discrimination perpetuated through AI systems.[492]

Unfortunately, this issue of bias in the healthcare application of AI is not uncommon. One study of a widely applied AI system in the healthcare sector in the US showed an example of racial bias perpetuated by an AI tool used in healthcare settings, wherein the stated goal of the AI tool was to identify patients who needed extra attention to their complex health needs. However, the unintended outcome of applying the AI tool was that it ascribed health costs as a proxy for health needs, which perpetuated a real-world racial bias and unfairness, as less money is typically spent on healthcare by Black patients who required the same level of care in comparison to their White counterparts, due to historical, socio-economic issues. The effect was that the algorithm falsely concluded that Black patients were healthier than equally sick White patients, resulting in sicker Black patients receiving similar care to healthier White patients despite needing the same or higher care.[493] Thus, the inherent bias adopted by the AI tool contributed to worse outcomes for Black patients by influencing the likelihood of receiving the appropriate level of care.

---

[488] Agarwal R et al, 'Addressing Algorithmic Bias and the Perpetuation of Health Inequities: An AI Bias Aware Framework' (2023) 12 *Health Policy and Technology*, 100702.

[489] Mittelstadt BD et al, 'The Ethics of Algorithms: Mapping the Debate' (2016) 3(2) *Big Data & Society* 1.

[490] Zou J, Schiebinger L, 'AI can be sexist and racist – it's time to make it fair' (2018) 559(7714) *Nature* 324.

[491] Chen I, Szolovits P, Ghassemi M, 'Can AI Help Reduce Disparities in General Medical and Mental Health Care?' (2019) 21(2) *The AMA Journal of Ethics* 167.

[492] Mehrabi N et al, 'A Survey on Bias and Fairness in Machine Learning' (2021) 54(6) *ACM Computing Surveys* 1.

[493] Obermeyer Z et al, 'Dissecting Racial Bias in an Algorithm Used to Manage the Health of Populations' (2019) 366 *Science* 447.

To prevent issues such as unfairness and bias caused by AI tools, developing nations should be cognizant of this issue of bias. The governments of these nations should incorporate intersectional justice to cater to more diverse, inclusive, and anti-colonial standpoints. This requires a commitment to imploring the development of a justice-oriented design of AI algorithims and AI-based support systems.[494] Developing nations should adopt technical and legal frameworks to minimize or prevent unfairness and bias. These laws should promote equity in the development process of AI tools applied to healthcare. To this end, AI tools that adopt a design rationale incorporating the principles of serendipity (diversifiability) and equity (intersectionality, reflexivity, and power balance) should be encouraged and adopted for creating healthcare AI tools.[495] The laws should also encourage developers of AI tools to adopt measures that limit bias and unfairness by adopting data pre-processing techniques, algorithmic modifications, or human oversight in AI decisions to create a fair society and reduce societal asymmetries and racial and gender stereotypes.[496]

Liability for harm

A significant legal challenge posed by the application of AI to promote the right to health in developing nations is the difficulty in detecting harm caused by algorithmic activity and finding its cause due to the black-box model of AI, which results in liability gaps. Liability gaps make it difficult to identify whom to ascribe responsibility and or liability for harm in situations where algorithmic activity causes damage to the patient accessing healthcare treatment, making it challenging to prevent it from happening again.[497]

There is a peculiar difficulty in ascribing responsibility for harm caused by the application of AI solutions in healthcare settings, primarily due to the myriad of actors responsible for administering healthcare to the individual and for developing and applying AI systems.

Take this instance for example: in determining who bears liability for harm caused to a patient due to the application of AI solutions to his healthcare needs, does the responsibility for harm caused lie with the healthcare practitioner, for instance, for not questioning the results of the AI tool that caused harm to the patient, even if they were unable to evaluate the quality of the diagnosis received from the AI tool against other sources of information, including their knowledge of the patient, due to the black-box nature of the AI system? Or is the responsibility for harm ascribed to the hospital or care facility due to its obligation to implement a policy allowing healthcare practitioners to overrule algorithmic advice? Or does the responsibility for harm lie with the commissioners or retailers of the system or device that contains the algorithm, as it may be argued that they bear some responsibility for checking the accuracy of decisions of the AI tool? Or does the responsibility for harm extend to the

---

[494] Baumgartner R et al, 'Fair and Equitable AI in Biomedical Research and Healthcare: Social Science Perspectives' (2023) *144 Artificial Intelligence in Medicine* 102658.

[495] Van Leeuwen C et al, 'Blind Spots in AI' (2021) 23 *ACM SIGKDD Explorations Newsletter* 42.

[496] Ibid., (Fn 36).

[497] Racine E, Boehlen W, Sample M, 'Healthcare Uses of Artificial Intelligence: Challenges and Opportunities for Growth' (2019) 32 *Healthcare Management Forum* 272.

national regulators for not appropriately assessing the product before it was deployed in healthcare settings in the country it was deployed in? Does this responsibility for harm also extend to the developers of the AI tool, for example, for inaccurate coding or poor-quality training data?[498]

It also needs to be determined who bears liability where the AI tools exhibit technical autonomy, wherein they act independent of human intervention due to their ability to learn independently and adaptation capacity, resulting in an unforeseeable output imagined by the parties mentioned above, including the developers themselves.[499]

From the preceding, it is evident that responsibility needs to be distributed, resulting in difficulties in ascribing blame for harm caused by actors in various parts of the healthcare delivery process wherein AI is applied. This lack of distributed responsibility results in difficulty in determining who to hold accountable for poor outcomes, which poses a significant risk to those seeking healthcare services wherein AI tools are adopted.

To answer the questions posed, developing nations need to take up solid regulatory frameworks that replicate or emulate the approach under international laws, such as the EU's administrative, regulatory approach to AI, which proposes to adopt an AI Act, a novel AI Liability Directive (AILD) in conjunction with a revised EU Product Liability Directive (PLD).[500] These laws constitute a proposed cornerstone of AI regulation and employ complementary approaches to regulating AI directly (via specific regulation in the AI Act) and indirectly (via incentives generated by the liability framework). The proposed AILD and PLD seek to integrate the AI Act into civil (product) liability to align the law with the new risks and realities this emerging technology poses.[501]

The proposed AI Act outlines a regulatory and oversight framework for AI systems, mainly those considered high-risk, to which AI tools developed and applied in healthcare settings belong, instituting obligations for creating and using them and banning specific harmful AI systems.[502] The proposed AI Act imposes strict liability on all operators and developers of these AI tools based on causation, which limits liability gaps.[503] Strict liability is used in the AI Act, with fault being the trigger for liability based on the tortfeasor's intent or negligence.[504]

Product defectiveness is the crucial requirement that triggers the producer's liability under the proposed PLD, which deals mainly with physical harm, including death,

[498] Morley J et al, 'The Ethics of AI in Health Care: A Mapping Review' (2020) 260 *Social Science & Medicine* 113172.

[499] Tessier C, *Robots autonomy: Some technical issues', Autonomy and Artificial Intelligence: A Threat or Savior?* (Springer, 2017), p. 180.

[500] European Commission, Proposal for a Directive of the European Parliament and of the Council on Liability for Defective Products, repealing Council Directive 85/374/EEC.

[501] Hacker P, 'The European AI liability directives – Critique of a half-hearted approach and lessons for the future' (*Cornell University*, 25 November 2022) <https://arxiv.org/abs/2211.13960> accessed 21 October 2023.

[502] European Commission, 'Document 52021PC0206: Proposal for a Regulation of the European Parliament and of The Council laying down harmonized rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts', 2021/206, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206>.

[503] Ibid., Art. 6.

[504] Deakin S, Adams Z, *Markesinis and Deakin's Tort Law* (8th edn, OUP, 2019), p. 87.

personal injury, or damage to the product or other property.[505] The proposed PLD defines a defective product "as a product that does not provide the safety the consumer is entitled to expect, considering all circumstances". It extends the party liable for harm from the 'producer' to the 'economic operator,' which is defined as "the manufacturer of a product or component, the provider of a related service, the authorized representative, the importer, the fulfillment service provider or the distributor," broadening the parties that may be liable for harm occurring to patients due to AI tools applied in their healthcare delivery.[506]

Notably, the notion of defect under the PLD only focuses on physical harm, excluding non-tangible harm that may occur, including privacy harm, cybersecurity flaws, or other risks. Thus, developing countries will have to adopt legal and regulatory frameworks that are cognizant of these non-tangible threats to individuals that may occur in the application of AI to promote access to healthcare.

Developing nations may adopt national policies that follow the proposed AILD, which seeks to lay uniform rules on the civil liability of owners and users of AI. The AILD complements the PLD and also follows the definition of high-risk in the proposed AI Act, detailing rules on the claimant's access to evidence of the defendant, allowing (potential) claimants to request access to relevant evidence about a specific high-risk AI system suspected of having caused damage.[507] The proposed AILD enables national courts to oversee and order the defendant's disclosure and preservation of evidence, and when a defendant fails to comply with court orders relating to the handling of evidence, a presumption of non-compliance with duties of care is presumed. However, the defendant may rebut the presumption by submitting evidence to the contrary.[508]

Developing nations may adopt the strict liability approach taken by the EU, which bridges responsibility gaps. However, it is essential to note that currently, many jurisdictions allow strict liability only for civil compensation of losses but not for criminal liability, as punishment under criminal law requires culpability. This may leave a gap in criminal responsibility for harm caused by the application of AI to healthcare services. Typically, States ascribe criminal responsibility compared to civil liability, to punish off enders rather than compensate victims and pursue further penological aims such as retribution or deterrence.[509] Developing nations seeking to apply AI tools to mitigate access to healthcare issues will need to adopt effective legal regulations that balance adequate compensation of injured persons criminal liability in situations that go beyond civil liability while balancing incentives for practical innovation and deployment of AI, to encourage the creation and adoption of AI tools that address access to healthcare issues. These incentives, however, should never come at the cost of unnecessary harm to individuals.

---

505 Article 6 (1) PLD proposal.

506 Article 7 PLD proposal.

507 Article 3 proposed AI Liability Directive.

508 Article 3(5) proposed AI Liability Directive.

509 Bublitz C and others, 'Legal Liabilities of BCI-Users: Responsibility Gaps at the Intersection of Mind and Machine?' (2019) 65 *International Journal of Law and Psychiatry* 101399.

Developing nations may also solve the issue of liability by dealing with the black-box model problem by mandating increased transparency and explainability of AI decisions. If healthcare practitioners can understand how a decision was reached, reflecting on an AI system's output becomes no different from any other diagnostic tool. If it can be proven that the duty of care was met, then the harm caused to a patient by an erroneous prediction of an AI-Health system would not constitute medical negligence.[510] However, it might also constitute negligence when healthcare providers fail to rely on the algorithmic output where the AI decision contains an obviously better treatment option for the patient.[511]

Conclusion and recommendation

This paper has attempted to show that although developing countries struggle with a high burden of disease, lack of trained healthcare providers, and poor healthcare delivery infrastructure, it is in these settings that AI has a tremendous potential to promote access to healthcare by reducing costs incurred due to accessing healthcare services, improving health equity, and improving the efficiency and quality of existing healthcare services. This technological advancement also improves existing healthcare systems, specifically in medical imaging and coronary artery disease diagnosis, by reducing human error, increasing patient care, and reducing the workload on healthcare professionals, which are currently reported as insufficient for the growing global populace. However, if the actual benefits of AI are to be gained, a collaborative approach should be encouraged between healthcare professionals and AI tools. As much as AI outperforms humans in data processing and analysis, human clinicians can exceed AI in the clinical decision-making process, as human clinicians have direct interactions with their patients and access to clinical and contextual information. Also, the qualitative data collected through clinician intuition plays a critical role in clinical decision-making, thus ensuring the safety of patients.[512]

The governments of developing nations should also be aware of the technological, ethical, and legal risks and challenges that arise when adopting AI, which must be addressed to ensure proper promotion of the right to health rather than perpetuating further harm. Meta-data generated from healthcare access, developed in the form of private sensitive and confidential information gathered in the process of healthcare delivery, is precious and priceless information that is required by the private companies who typically develop and run most AI tools, as such, securing this data is of vital importance and should be appropriately protected.

Developing countries should be included in adopting this emerging technology as it has the potential to address many of the infrastructural deficits that currently plague

[510] Holzinger A, Haibe-Kains B, Jurisica I, 'Why Imaging Data Alone Is Not Enough: AI-Based Integration of Imaging, Omics, and Clinical Data' (2019) 46 *European Journal of Nuclear Medicine and Molecular Imaging* 2722.

[511] Schönberger D, 'Artificial intelligence in healthcare: a critical analysis of the legal and ethical implications' (2019) 27(2) *Int. J. Law Info Technol.* 171.

[512] Chen A, Wang C and Zhang X, 'Reflection on the Equitable Attribution of Responsibility for Artificial Intelligence-Assisted Diagnosis and Treatment Decisions' (2023) 3 *Intelligent Medicine* 139.

the healthcare sectors of many of these countries. The governments of developing countries like Nigeria in particular, should seriously encourage the adoption of this technology in its public health sector as a solution to its human resource constraints, as its national populace continues to soar compared to its healthcare worker population, which continues to dwindle.

Developing countries will also need to address their other prevailing socio-economic challenges, which may hamper the uptake of developing and applying AI tools. These include issues relating to the infrastructural deficits required for AI systems, including constant electricity supply and high-powered internet. The nations also need to focus on developing policies and securing sustained financing for these emerging technologies to bloom to ensure their long-term success, which is required to digitize healthcare and AI developments. The regulatory framework that is to be developed to regulate AI tools should also take cognizance of existing criminal and civil laws while ensuring a just application of AI tools, preventing instances of perverted use of AI tools, including introducing social policing and other unfair practices, as may be seen in some countries in the world today.

Addressing these issues and adopting the recommendations in this paper can impact the lives of many individuals and accelerate access to healthcare by properly adopting AI to address the challenges developing nations currently face regarding their healthcare sector. These countries may wish to adopt the recommendations in this paper to tackle these issues. However, these countries should be cognizant of their distinct national peculiarities and, as such, tailor their AI regulation and application to healthcare to accommodate this fact.

4.3 EU Cyber Sanctions: Current International Legal Controversies and Future Prospects

By ***Nicolas Sabján*** (Comenius University Bratislava)

Introduction

We live in the "age of sanctions". The relevant sanctions databases show the steep increase in the imposition of sanctions since the end of the Cold war[513] and the EU has contributed significantly to this state of affairs. Hence the description of the EU as a "sanctioning power".[514]

Combined with this, a further phenomenon is digitalisation that has had a profound effect on every aspect of our societies, including public international law. It is precisely digital technologies and their effect that led to the decision of some states to create a relatively new cyber sanctions regime as a specific reaction to these changes.

Another feature of our current predicament is the profound geopolitical change that has been taking place after the End of history period of 90's. Starting with the first point, we have arguably entered a period of multipolarity,[515] characterised by the shift of power from the West to the 'Rest', or some sort of convergence. Secondly, many have pointed out that this multipolarity entails a geo-economic element, i. e. the economisation of security and securitisation of economy.[516] In a somewhat similar description, Mark Leonard contends that we live in an age of 'unpeace',[517] which is a particularly apt description for cyberspace. Furthermore, weaponisation of interdependence is expanding, for instance in the form of (cyber) sanctions. Indeed, interdependence is in a sense a necessary condition for the successful and effective imposition of sanctions. The background condition that gives rise and co-determines the abovementioned is the ongoing great power competition. Without making this condition inevitable or deterministic, we agree with the claim that great-power competition has not returned (as it is often argued), because it never actually went away.[518]

Against this background, we shall explore in this article the intersection of the three abovementioned trends that are unfolding on the international level, while laying emphasis on the phenomenon of digitalisation and its relationship to sanctions law (focusing on EU cyber sanctions), whilst discussing some of the international legal

[513] Felbermayr G et al, 'The Global Sanctions Data Base' (2020) 129 *European Economic Review* 1.

[514] With several country-specific and thematic sanctions in place. See E EU Sanctions Map <https://www.sanctionsmap.eu/#/main> accessed 31 December 2023.

[515] Acharya A, Estevadeordal A and Goodman LW, 'Multipolar or Multiplex? Interaction Capacity, Global Cooperation and World Order' (2023) 99 *International Affairs* 2339.

[516] Roberts A, Choer Moraes H, Ferguson V, 'Toward a Geoeconomic Order in International Trade and Investment' (2019) 22 *Journal of International Economic Law* 655.

[517] Leonard M, *The Age of Unpeace: How Connectivity Causes Conflict* (Penguin, 2022).

[518] Nexon DH, 'Against Great Power Competition' (*Foreign Affairs*, 26 June 2023) <https://www.foreignaffairs.com/articles/united-states/2021-02-15/against-great-power-competition> accessed 31 December 2023.

aspects of it. Accordingly, the article is divided into three parts. First, we outline the legal framework of EU cyber sanction, its nuances and specificities. Secondly, we shall focus on the question of immunity law that might come to the fore in the context EU cyber sanctions which entail the imposition of asset freezes on state officials or government agencies. Finally, the article will discuss several different aspect of digitalisation (including new technologies) and its effects on the field of sanctions. Our aim in this is to critically reflect on the perspicuous analysis put forward by Dana Burchardt, who recently discussed the question whether digitalization is changing international law *structurally*.[519] In particular, we shall focus on the possible consequences of digitalization on the field of sanctions law.

1. Outlining the EU Cyber-Sanctions Regime

The cyber sanctions framework adopted by the European Union (hereinafter "EU") represents a relatively recent foreign policy tool in the context of cyber security. It came into effect in 2019 in the form of a Council Decision (CFSP) 2019/797 and Council Regulation 2019/796 that sets out the conditions for imposing restrictive measures against cyber-attacks. Cyber sanctions fall under the rubric of horizontal sanctions (together with other horizontal restrictive measures in the context of terrorism, human rights, chemical weapons…) and are targeted in nature (so-called "smart sanctions"), as opposed to country-specific measures that are normally more comprehensive.[520]

The objective of EU cyber sanctions is to "*respond to and deter cyber-attacks with a significant effect which constitute an external threat to the Union or its Member States*."[521] Hence, cyber sanctions are to be regarded as deterrence[522] measures, while by and large, restrictive measures also aim to change the behaviour of states (in this case, within the context of cyberspace). However, the EU does not characterise these measures as a "punishment" though there is a thin line between "responding to" some malicious cyber activity and punishment. Beyond this, there is an obvious signalling effect too, similarly as in the case of "traditional" sanctions. The paradox however is that there has been practically no direct attribution to any state from the EU as such which is potentially counterproductive and could limit the deterrent effect of cyber sanctions (it is well-known that different States were involved in many cyber-attacks). Moreover, when cyber sanctions were imposed by the EU, for instance in the WannaCry and NotPetya cases, it took two years from the official

[519] See, Burchardt, D, 'Does Digitalization Change International Law Structurally?' (2023) 24 *German Law Journal* 438.

[520] Lonardo L, *EU Common Foreign and Security Policy after Lisbon between Law and Geopolitics* (Springer, 2023), p. 74.

[521] Council of European Union, Council Regulation (CFSP) 2019/796 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States.

[522] However, it must be admitted that the deterrence effect of cyber sanctions is not supported by empirical evidence. See, Sameer Patil, 'Assessing the Efficacy of the West's Autonomous Cyber-Sanctions Regime and Its Relevance for India: EU Cyber Direct' (*Horizon*) <https://eucyberdirect.eu/atlas/sources/assessing-the-efficacy-of-the-west-s-autonomous-cyber-sanctions-regime-and-its-relevance-for-india> accessed 31 December 2023.

condemnation.[523] It should be emphasized that cyber sanctions are only one of the tools with which the EU responds to malicious cyber-attacks, with the knowledge that these measures might not be sufficient and effective.

According to Article 1 (2) (c) of the Regulation, a wide range of subjects can be targeted with cyber sanctions (in essence, any kind of subject).[524] Among other things, the Regulation permits the imposition of cyber sanctions even in cases of cyber-attacks against third states and international organizations.[525] The restrictive measures that can be imposed include travel bans, asset freezes and the prohibition to make funds and economic resources available to subjects accused of cyber-attacks.[526]

Horizontal sanctions, in particular cyber sanctions, gives the Council a relatively wide leeway due to the indeterminate formulations used in the relevant Regulation.[527] Cyber sanctions might be imposed not only against 'classical' cyber-attacks, but arguably in cases of economic espionage or other theft in the cybersphere.[528] Moreover, the adoption procedure of cyber sanctions is more flexible since it is not required to enact a new legal framework each time the listing is to be updated, thereby avoiding the tedious procedure connected with the country-specific restrictive measures. In addition, in the case of horizontal sanctions, attribution questions do not have to be dealt with (at least not directly), since "*targeted restrictive measures should be differentiated from the attribution of responsibility for cyber-attacks to a third state. The application of targeted restrictive measures does not amount to such attribution, which is a sovereign political decision.*"[529]

It was most likely an intention to avoid questions regarding attribution in light of state responsibility norms under international law (ARSIWA) which is a highly contentious issue, especially in the cyberspace context. Nevertheless, we agree with the claim of Yuliya Miadzvetskaya and Ramses Wessel that imposing restrictive measures on individuals is often an indirect attribution to states (since the sanctions subjects are in some cases government officials[530]) even if the EU does not formally recognizes

---

[523] Bendiek A and Schulze M, 'Attribution: A Major Challenge for EU Cyber Sanctions' (*Stiftung Wissenschaft und Politik (SWP)*) <https://www.swp-berlin.org/10.18449/2021RP11/> accessed 31 December 2023, p. 26.

[524] "*Cyber-attacks constituting an external threat include those which: (c) are carried out by any natural or legal person, entity or body established or operating outside the Union; or (d) are carried out with the support, at the direction or under the control of any natural or legal person, entity or body operating outside the Union.*"

[525] Council of European Union, Council Regulation (CFSP) 2019/796 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States, Article 1(6).

[526] Ibid., Art. 3.

[527] See *infra.*

[528] Bogdanova I and Vásquez Callo-Müller M, 'Unilateral Cyber Sanctions: Between Questioned Legality and Normative Value' (2021) 54 *Vanderbilt J. Transnat'l L.* 4, p. 931. There have been several incidents of economic espionage carried out also against EU states (however, it is more discussed in the US context). See, Cristani F, 'Economic Cyber-Espionage in the Visegrád Four Countries: A Hungarian Perspective' (2021) 17 *Politics in Central Europe* 697; Market D-G for I and PwC, 'The Scale and Impact of Industrial Espionage and Theft of Trade Secrets through Cyber' (*Publications Office of the EU*, 2018) <https://op.europa.eu/en/publication-detail/-/publication/4eae21b2-4547-11e9-a8ed-01aa75ed71a1> accessed 31 December 2023.

[529] Council of European Union, Council Decision (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member State.

[530] Examples are four Russians of the GU/GRU, including the Head of the Main Directorate; Chinese and

the act as such.[531] Factually, in many cases there were links between the perpetrators of cyber-attacks and different governments and were not carried out individually (StuxNet, WannaCry, NotPetya, the attempted attack against OPCW).[532]

As to the issue of vagueness, the Regulation enables the adoption of cyber sanctions against "*cyber-attacks with a significant effect*" that could have "*a potentially significant effect which constitutes an external threat to the Union or its member states*."[533] The term "significant" effect is open-ended and ensures much flexibility, albeit Article 2 lists several factors that shall be taken into account when assessing the significance of the attack.[534] The same applies to the term "external threat". The latter term is specified in Article 1 (4) of the Regulation, though the list set out therein is not exhaustive. Such vagueness could be justified by the need to ensure a certain degree of flexibility for the Union to react promptly and more effectively in the cyberspace, which is unpredictable and subject to permanent change. Moreover, the Council had taken heed of the decision-making of the Court of Justice that has a relatively strong role in the context of restrictive measures.[535] The Council took a lesson from past judicial practice where it could not defend some of the restrictive measures it imposed.[536] On the other hand, the vagueness and imprecise nature of listing criteria creates the possibility for arbitrary decision-making, disregarding the principle of legal certainty.

The second point concerns evidentiary issues. The listing must not only be based on specific reasons, but it shall be supported by evidence. Moreover, to ensure the right to fair trial the listed individuals must have access to this evidence.[537] This procedural

North Korean state-sponsored groups specializing in cyber operations. See: Annex, Council of European Union, Council Decision (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member State.

531 Miadzvetskaya Y, Wessel AR, 'The Externalisation of the EU's Cybersecurity Regime: The Cyber Diplomacy Toolbox' (2022) 7 *European Papers* 413, p. 435.

532 Miadzvetskaya Y, 'Cyber sanctions: towards a European Union cyber intelligence service?' (*College of Europe Policy Brief*, 2021) <https://www.coleurope.eu/sites/default/files/research-paper/miadzvetskaya_cepob_1-2021_final_0.pdf>. Currently, there are four entities and eight individuals that are on the cyber sanctions list. See, Council of the European Union, Cyber-attacks: Council extends sanctions regime until 18 May 2025, Press release, <https://www.consilium.europa.eu/en/press/press-releases/2022/05/16/cyber-attacks-council-extends-sanctions-regime-until-18-may-2025/> accessed 31 December 2023.

533 Council of European Union, Council Regulation (CFSP) 2019/796 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States, Article 1(1).

534 "*The factors determining whether a cyber-attack has a significant effect as referred to in Article 1(1) include any of the following: (a) the scope, scale, impact or severity of disruption caused, including to economic and societal activities, essential services, critical State functions, public order or public safety; (b) the number of natural or legal persons, entities or bodies affected; (c) the number of Member States concerned; (d) the amount of economic loss caused, such as through large-scale theft of funds, economic resources or intellectual property; (e) the economic benefit gained by the perpetrator, for himself or for others; (f) the amount or nature of data stolen or the scale of data breaches; or (g) the nature of commercially sensitive data accessed.*"

535 Chachko E, 'Foreign Affairs in Court: Lessons from CJEU Targeted Sanctions Jurisprudence' (2019) 44 *Yale Journal of International Law* 1, p. 2.

536 Miadzvetskaya Y, 'Cyber sanctions: towards a European Union cyber intelligence service?' (*College of Europe Policy Brief*, 2021) <https://www.coleurope.eu/sites/default/files/research-paper/miadzvetskaya_cepob_1-2021_final_0.pdf>, p. 3.

537 Gordon R, Smyth M and Cornell T, *Sanctions Law* (Hart, 2019), pp. 156–163.

requirement is even more problematic in the case of cyber sanctions due to the fact that the cyberspace is in principle an anonymous sphere where obtaining relevant evidence is not without difficulties. Thus, attribution of cyber-attacks to particular actors to establish the necessary nexus might be problematic, even if the evidentiary standards are of a lower threshold (sufficiently solid factual basis) as opposed to the one in criminal cases (beyond reasonable doubt).

Furthermore, no less problematic is the fact that the evidence in cyber context is essentially confidential, normally provided by the intelligence authorities of the specific member state. However, member states may decline to share the evidence with the Council for national security reasons in light of the rule of originator control. In fact, there have already been cases in which the member states refused to share the intelligence data for sanctions listings.[538]

By and large, the main problems with respect to cyber sanctions could be summarised in the following way: first, the presence of issues of transparency and procedural rights; second, and in connection with the first issue, the lack of intelligence sharing prevents a proper justification during judicial review; third, inconsistencies in the application of cyber sanctions – in the case of Bundestag hack and Cloud Hopper (where espionage was involved) restrictive measures were imposed, whereas in other similar cases the EU refrained from taking any action[539]; four, as seen in the WannaCry and NotPetya cases, the speed of imposition could compromise the effectiveness of sanctions.[540]

With respect to the consequences of cyber sanctions imposed by the EU (or other states, such as US, UK…) for international law, they constitute relevant state practice and do contribute to the development of rules of international law, in particular in the field of customary international law. As Iryna Bogdanova and Callo-Muller contend, the imposition of cyber sanctions could be understood as "*signalling red lines in cyberspace. Thus, cyber sanctions should be studies: they could substantiate the crystallization of customary international law regarding responsible state behaviour in cyberspace*."[541] In the next part, we shall look into the unresolved question from the perspective of international legal norms.

[538] Miadzvetskaya Y, 'Cyber sanctions: towards a European Union cyber intelligence service?' (*College of Europe Policy Brief*, 2021) <https://www.coleurope.eu/sites/default/files/research-paper/miadzvetskaya_cepob_1-2021_final_0.pdf>. There is indeed a growing call for more effective coordination between the intelligence agencies of member States, cooperation between the EU and private sector or even a more ambitious proposal to create an EU intelligence authority.

[539] See e.g., Soesanto S, 'After a Year of Silence, Are EU Cyber Sanctions Dead?' (*Default*, 26 October 2021) <https://www.lawfaremedia.org/article/after-year-silence-are-eu-cyber-sanctions-dead> accessed 31 December 2023.

[540] Bendiek A and Schulze M, 'Attribution: A Major Challenge for EU Cyber Sanctions' (*Stiftung Wissenschaft und Politik (SWP)*) <https://www.swp-berlin.org/10.18449/2021RP11/> accessed 31 December 2023, pp. 34–36.

[541] Bogdanova I and Vásquez Callo-Müller M, 'Unilateral Cyber Sanctions: Between Questioned Legality and Normative Value' (2021) 54 *Vanderbilt J. Transnat'l L.* 4, pp. 922–923.

2. International Legal Aspects of EU Cyber Sanctions – Immunity Law

Cyber sanctions raise several issues from the perspective of international legal norms, immunity law being one of them.[542] One of the measures imposed in the context of cyber sanctions are asset freezes, which raises the question of immunity from jurisdiction/enforcement of States and its property in light of UNCSI (reflected as customary international law). First, according to Article 2(1)(a) of the UNCSI, the term "state" includes also "*agencies or instrumentalities of the State*", other entities that are exercising sovereign authority of the State and also state officials.

As already set out at above, EU cyber sanctions are imposed against state officials (and could be imposed against government agencies) that are undertaking *de jure imperii* functions. These restrictive measures fall into the category of financial sanctions (asset freezes), clearly affecting the property of these high state officials or government agencies, i. e. it can be said to constitute "measures of constraint".[543] This much is not disputed as financial sanctions (in our case, asset freezes) are inherently constraining due to the fact that the individual cannot freely dispose with his or her property. However, as Tom Ruys observes, "*the question arises whether the circumstance that the property of a foreign* State or *its officials is being 'affected' and the 'constraining' nature of the sanctions suffices to trigger the application of the relevant immunity rules*."[544]

Now it is widely accepted that customary international law (as the UNCSI is not in force yet) distinguishes immunity from jurisdiction (protection from the civil and criminal jurisdiction of foreign States) and immunity from enforcement (protection from enforcement measures of a foreign State). Having said this, the restrictive measures imposed by the EU (including cyber sanctions) do not have a criminal character as mentioned above, but are administrative measures that are temporary (though in some cases, the asset freezes are in place for a rather long period). In any case, it may appear that asset freezes are clear violation of immunity from enforcement. However, the issue is somewhat more complicated and far from settled. The argument against this conclusion goes as follows: even though immunity of enforcement is clearly established under customary international law and asset freezes (or other acts) are deemed to be measures of constraint, this immunity only applies in connection with court proceedings, i. e. in line with the UNCSI, pre-judgmental or post-judgment measures of constraints are covered by immunity law. We can further support this argument with other international instruments, e. g. the European Convention on State Immunity, the domestic legislation of US (United States 1976 Foreign Sovereign Immunities Act), UK (1978 State Immunity Act), as well as other states (Australia, Canada, Singapore, Argentina) or the scholarly work concerning the issue at hand.[545] All of the legal materials cited are formulated in a similar way, that is, immunity is linked to

[542] Ibid.

[543] UNGA, 'United Nations Convention on Jurisdictional Immunities of States and Their Property', A/RES/59/38 (2004), Art. 18.

[544] Ruys T, 'Immunity, Inviolability and Countermeasures – A Closer Look at Non-UN Targeted Sanctions' in Ruys T, Angelet N and Ferro L (eds), *The Cambridge Handbook of Immunities and International Law* (CUP, 2019), p. 676.

[545] Ibid.

court proceedings. This conclusion might seem a bit counterintuitive, but the primary legal materials quite clearly signal that the nexus to court proceeding is inevitable (this interpretation is also supported by scholarship).[546] If we accept this interpretation, it would mean that asset freezes, normally adopted by executive organs without any involvement of court proceedings, do not violate customary immunity rules.

A counter-argument invokes the sovereign equality of States as a basic principle from which state immunity is deduced.[547] Consequently, immunity from enforcement cannot be limited to court proceedings since this would severely restrict state immunity applicable to its property and violated the principle of sovereign equality. The problem with this argument is that the principle of sovereign equality is indeterminate and the abovementioned conclusion does not clearly stem from it.

Another objection could be made on the basis of extensive interpretation of the term "court" stipulated in Article 2(1)(a) UNCSI. It is defined as "*any organ of a State, however name, entitled to exercise judicial functions*." The ILC Commentary then elaborates further on the term judicial functions:

> *"Judicial functions may be exercised in connection with a legal proceeding at different stages, prior to the institution or during the development of a legal proceeding, or at the final stage of enforcement of judgements. Such judicial functions may include adjudication of litigation or dispute settlement, determination of questions of law and of fact, order of interim and enforcement measures at all stages of legal proceedings and such other administrative and executive functions as are normally exercised by, or under, the judicial authorities of a State in connection with, in the course of, or pursuant to, a legal proceeding. Although judicial functions are determined by the internal organizational structure of each State, the term does not, for the purposes of the present articles, cover the administration of justice in all its aspects which, at least under certain legal systems, might include other functions related to the appointment of judges."*[548]

Again, judicial functions are linked with court proceedings, as we can see from the excerpt of ILC Commentary. At the same time, it is true that in a different part, ILC seems to give a more extensive interpretation, noting that judicial functions "*may, under different constitutional and legal systems, cover the exercise of the power to order or adopt enforcement measures (sometimes called "quasi-judicial functions") by a specific administrative organ of the State*."[549]

Thus, the question remains whether EU restrictive measures (in our case asset freezes), adopted by the Council in the form of a decision/regulation, could be qualified as a "quasi-judicial function". Since there is a paucity of judicial practice in this regard,

---

[546] See e.g., Brunk I, 'Central Bank Immunity, Sanctions, and Sovereign Wealth Funds' (2023) 91 *George Washington Law Review* 1616.

[547] The argumentation is more developed in Ruys T, 'Immunity, Inviolability and Countermeasures – A Closer Look at Non-UN Targeted Sanctions' in Ruys T, Angelet N, and Ferro L (eds), *The Cambridge Handbook of Immunities and International Law* (CUP, 2019), pp. 684–686.

[548] ILC, 'Draft Articles on Jurisdictional Immunities of States and Their Property, with commentaries 1991' (1991), p. 14.

[549] Ibid.

the issue remains unresolved for now. Our view is that EU restrictive measures as such do not impinge on immunity law as there is essentially no connection whatsoever to court proceedings. By contrast, if the assets were to be seized, this would inevitably involve court proceedings, since this is legally required under European human rights law and therefore, immunities must be respected.[550]

3. Implications of New Technologies/Digitalization for Sanctions Law

In this part, we discuss the implication of digitalization and new technologies for the international legal field. The fast-paced developments of in the technological sphere make it rather difficult to explain all the possible consequences and even the adoption of proper legislative framework is not without difficulties. Nonetheless, several repercussions for the field of sanctions law and international law more generally (we shall focus on the former) could be identified.

Let us start with the contention that by and large, sanctions are imposed by more powerful states, having the economic, political, administrative etc. capacity to adopt such measures. That is the reason why sanctions are perceived rather critically in the Global South and by scholars associated with TWAIL or other critical approaches, characterising sanctions as an imperial tool, a tool against the weak.[551] Cyber sanctions, as a reaction to the growing number of malicious cyber-attacks, extend the already mentioned extensive list of sanctions and could further entrench inequalities between states. This is the gist of the argument put forward by Dana Burchardt. Let us discuss it in more detail.

First, the establishment of cyber sanctions legal framework is the domain of just a few states with the capacity (technical, administrative, legal, etc.), necessary resources and expertise. Currently, such legislative framework was enacted, for instance by US, EU, UK. Consequently, these states are in a privileged position, being the "norm/standard-setters". This then creates the basis for other imbalances, i. e. these states will have the power to create and shape state practice regarding cyber sanctions. Furthermore, the very same dynamic is pertinent in contentious issues related to sanctions. For instance, in the context of attribution, factual assessments must be made, presupposing sufficient technical capabilities and expertise before any application of legal rules actually comes into consideration. Thus, the development of international rules concerning state responsibility (which is often connected with sanctions since these can be justified as countermeasures) is mostly in the hands of powerful states or group of states, e.g. the EU.[552] Moreover, these possible imbalances/inequalities in regard to technical capabilities and attribution in general also exist among the EU countries as such.

---

[550] Brunk I, 'Central Bank Immunity, Sanctions, and Sovereign Wealth Funds' (2023) 91 *George Washington Law Review* 1616.

[551] See e.g., 'Symposium: Third World Approaches to International Law (TWAIL) & Economic Sanctions' (*Yale Journal of International Law*, 20 September 2020) <https://www.yjil.yale.edu/symposium-third-world-approaches-to-international-law-economic-sanctions/> accessed 31 December 2023.

[552] Poli S, Sommario E, 'The Rationale and the Perils of Failing to Invoke State Responsibility for Cyber-Attacks: The Case of the EU Cyber Sanctions' (2023) 24 *German Law Journal* 522.

We might add to this that an important aspect in the context of attribution is the role of private sector. Private cybersecurity companies play a particularly crucial role due to their technological capability and expertise (e. g. computer forensic capabilities).[553] As pointed out by experts in the field, "*some of the most influential reports linking malicious cyber operations to governments and non-state actors have been released by private companies*."[554] Indeed, he concludes that the public-private relationship in the field of cyber sanctions (EU and private companies) has been reversed and the former is by now much more dependent on the latter than *vice versa*. In reality then, "*governments rely on the private sector for forensic and strategic information, thereby turning the security companies into quasi-intelligence services*."[555] It is mostly Western countries where these private companies are located and thus, the governments (or the EU in our case) is able to harness the capabilities and expertise of these actors, thus having the potential for contributing to the development of state responsibility (attribution for instance).

On the other hand, we claim that there is a formidable challenge to this practice by a large number of states mainly from the Global South, together with powerful states like China or Russia.[556] Moreover, cyber sanctions are often imposed precisely against cyber-attacks or other malicious cyber activity perpetrated by the abovementioned states that are simultaneously (formally) critical towards the sanctions practice.[557] Furthermore, in the context of attribution, other considerations are present also. States, having the capacity to make the technical determination and attributing cyber-attacks to other states rarely do that, for political and strategic reasons. Although it shall be recognised, that these states still have the *capability* to do that.

Subsequently, we claim in this regard that digitalization or the emergence of new technologies may empower also less powerful states in the context of great-power competition. It is recognized that some of the new technologies could be rather "efficient", i. e. causing significant damage and being effective as a tool of asymmetric warfare. One indication that supports this contention is the transformation of argumentative practices of states.[558] It seems to be the case that the principle of non-intervention and sovereignty in the cyberspace is being more often invoked by more powerful states. Traditionally, these kinds of arguments based on the said principles were used by weaker states against the intrusion

---

[553] Pawlak P and Biersteker TJ, 'Guardian of the Galaxy. Eu Cyber Sanctions and Norms in Cyberspace' (*Graduate Institute of International and Development Studies*, October 2019) 70 <https://repository.graduateinstitute.ch/record/298089?_ga=2.189322283.1057064273.1704068666-773194854.1704068666> accessed 31 December 2023.

[554] Ibid., p. 71.

[555] Ibid., p. 75.

[556] The fact however is that China and Russia's opposition to sanctions is purely formalistic, taking this position only due to strategic and geopolitical reasons. This can be clearly seen from their practice – both China and Russia have imposed sanctions on several occasions and continue to do so. See chapters 5 and 6 in Beaucillon C, *Research Handbook on Unilateral and Extraterritorial Sanctions* (Elgar, 2021).

[557] As stated above, even though some of the cyber-attacks were not officially attributed to Russia or China by the EU, several analyses confirmed this. Furthermore, cyber sanctions were imposed against foreign state officials (e.g. GRU officials).

[558] Burchardt D, 'Does Digitalization Change International Law Structurally?' (2023) 24 *German Law Journal* 438.

in different forms in their internal and external affairs.[559] This example show the way how the power-balance is upset and is being shaped by the new technologies and digitalization.

In sanctions law, this dynamic has already materialized in different ways. For instance, new technologies are employed to circumvent sanctions imposed often by powerful states as state above.[560] Digital currencies or blockchain technology are most relevant in this respect – the decentralised and anonymous nature of such technologies could make it rather difficult to prevent sanctions-evasion. It is very likely that these technological advances will fundamentally alter the field of sanctions, albeit one has to admit that currently, in many instances, the imposition of sanctions is still effective. Additionally, these 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.

In any case, the analysis concerning the imbalances/inequalities that we mentioned above should be more nuanced as digitalization is in some respect janus-faced. It is not merely a tool/instrument for powerful states to further consolidate the actual power-structure on the international level but on the contrary, the existing order might even be in some cases upended and challenged.

Secondly, it is argued that the nature of rules is affected by digitalisation, including the legal framework on sanctions. In particular, the claim is that we moving towards a structural change in the context of legal norms, resulting in the "flexibilization of rules".[561] This contention is warranted and we argued above that the EU cyber sanctions regime is also characterized by it. As explained above, the relevant Regulation on cyber sanctions is vague and open-ended, giving the Council a wide discretion. On the one hand, due to the rapid development of technologies which might then be deployed in the future for malicious purposes partly justifies this flexibilization, since in some cases it is vital to react in a sufficient manner. It shall be emphasized nonetheless that even if this sort of indeterminacy is not alien to international legal rules, the danger of abuse looms large.

A simultaneous trend specific for the cyber field is informalization,[562] relevant for cyber sanctions as well. This informalization is connected with the growing role of private actors in the digital sphere when it comes to norm-setting power and cyber sanctions. Self-regulatory initiatives by private actors are expanding, having an informal character, including different codes of conduct, non-binding documents *et cetera*.[563] A certain risk

---

[559] This can be seen in other context too. See for instance: Nguyen A, 'The G7's Fear of Economic Coercion through Weaponised Interdependence – Geopolitical Competition Cloaked in International Law?' (*EJIL*, 22 June 2023) <https://www.ejiltalk.org/the-g7s-fear-of-economic-coercion-through-weaponised-interdependence-geopolitical-competition-cloaked-in-international-law/> accessed 31 December 2023.

[560] Demarais A, *Backfire: How Sanctions Reshape the World against U.S. Interests* (Columbia University Press, 2023); Abusedra A, Bakar A, Islam MT, 'Use of Cyber Means to Enforce Unilateral Coercive Measures in International Law' in Subedi SP (ed), *Unilateral Sanctions in International Law* (Hart, 2022).

[561] Burchardt D, 'Does Digitalization Change International Law Structurally?' (2023) 24 *German Law Journal* 438, pp. 448–449.

[562] Ibid.

[563] Pawlak P and Biersteker TJ, 'Guardian of the Galaxy. Eu Cyber Sanctions and Norms in Cyberspace' (*Graduate Institute of International and Development Studies*, October 2019) <https://

exists with the growth of these informal rules as these could cause an overlap with binding rules whereby the latter's binding nature is transformed and its bindingness gradually hollowed out.[564] The adoption of non-legal documents has not occurred yet in sanctions law, but there are other ways through which it is "colonized" by these informal rules. In particular, relatively powerful private actors are employing instruments that have *de facto* sanctions effect (for instance limiting access to services and products that are provide by them) whose "legal" basis are precisely these informal rules.[565] This is frequently undertaken in cooperation with law enforcement organs of the state. Such trend may result in circumventing the rules on cyber sanctions, giving preference to 'informal regimes' where the international legal framework is even more blurred.

Thirdly, two interconnected phenomena can be observed with respect to the issue of digitalisation and international law – regionalization and fragmentation.[566] In some sense, the former is the cause of the latter. Starting with regionalization, it appears that a divide between Western and non-Western states is being crystallized. A well-known example is the discord between the two groups of states in connection with the rules on cyberspace in the UN.[567] Cyber sanctions are equally regionalized, albeit it is not merely cyber sanctions but sanctions law as such. As pointed out before, there is a divide between Global South/North on the legality of unilateral sanctions and thus, the regional character of sanctions law is not an entirely unprecedented change.

The regional character of rules on digitalization creates and fuels fragmentation of international law. If the rules on cyberattacks, principle of non-intervention, human rights and other issues related to digitalization are not unified and are interpreted and applied differently in different regions, how is it possible to establish attribution and the violation of international norms that serve as a basis to react by imposing sanctions in a legally acceptable manner?

A distinct way to conceptualize the fragmentation created by digitalization, according to Burchardt, is the divide between the digital and non-digital legal regimes.[568] It is not clear yet whether we can see some sort of 'paradigmatic shift' which will establish parallel sanction law regimes in the digital and non-digital sphere. Currently, this does not seem to be the case due to the fact that the EU has failed to employ the cyber sanctions regime more actively, even though there were several occasions where EU was an object of malicious cyber practices.[569] Be that as it may, we may contend nevertheless

---

repository.graduateinstitute.ch/record/298089?_ga=2.189322283.1057064273.1704068666-773194854.1704068666> accessed 31 December 2023, pp. 74–75.

564 Burchardt D, 'Does Digitalization Change International Law Structurally?' (2023) 24 *German Law Journal* 438, p. 449.

565 Pawlak P and Biersteker TJ, 'Guardian of the Galaxy. Eu Cyber Sanctions and Norms in Cyberspace' (*Graduate Institute of International and Development Studies*, October 2019) <https://repository.graduateinstitute.ch/record/298089?_ga=2.189322283.1057064273.1704068666-773194854.1704068666> accessed 31 December 2023, p. 75.

566 Burchardt D, 'Does Digitalization Change International Law Structurally?' (2023) 24 *German Law Journal* 438, p. 450.

567 Ibid., p. 449.

568 Ibid.

569 See, supra (n 540).

that cyber sanctions with its specificities and distinctive nature (as discussed above) as compared to 'traditional' sanctions were a direct result of the emergence and deployment of new technologies. In this sense, there is already a *de facto* divergence between digital/non-digital sphere to some degree and we shall see if this fragmentation will intensify.

Fourthly, it is hardly surprising that digitalisation/new technologies as novel developments caused a paucity in the international legal field. There is ambiguity or uncertainty regarding the legal regulation of cyberattacks or other aspects of the cyber space, as explained above. The relatively new cyber sanctions regime is also a case in point. The legal paucity in situations of novel societal or technological developments is, more often than not, deliberately maintained for strategic and political reasons.[570] The EU or other sanctioning powers seem to prefer the *status quo,* which gives them a degree of flexibility, being wary of committing to international rules that might, at the end of the day, be a limiting factor. On the other hand, middle and emerging powers could harness this uncertainty in the cyberspace too, which shows again the janus-faced character of these developments. Thus, the argument regarding the maintenance and reproduction of inequalities (see above) is not that straightforward.

Conclusion

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. This article aimed to expand and contribute to some aspects of the discussion on the relationship between digitalisation/new technologies and international law, focusing in particular on EU cyber sanctions regime, a relatively new phenomenon closely connected to the rise of new digital technologies.

Let us sum up some of the conclusion(s) and *future prospects*. First, we discussed some of the specificities but also problems with regard to EU cyber sanctions. From the international legal perspective, we focused on the question of immunity law that remains unresolved for now, as there is no relevant judicial practice.

In general, we outlined the janus-faced character of new digital technologies in the context of sanctions (i. e. there is a potential to undermine the effectivity of sanctions, while these tools could be in the future deployed to more effective enforcement).

Furthermore, we critically assessed some of the arguments made by Dana Burchadt concerning the entrenchment of existing inequalities due to digitalization. We argued that the picture is more nuanced due to the ongoing shifts in the power-structure on the international level and the indeterminate character of, in our case, EU cyber sanctions regime, and the cyberspace more generally.

So, what are the future prospects? In that regard, we propose that the imposition of cyber sanctions will not wither away and may even increase as a response to malicious cyber activities There are two reasons for this: first, there is a high probability that malicious cyber activities will increase, considering the current geopolitical tension between the US, EU, China and the emerging new powers, and furthermore, an ever-

[570] Poli S, Sommario E, 'The Rationale and the Perils of Failing to Invoke State Responsibility for Cyber-Attacks: The Case of the EU Cyber Sanctions' (2023) 24 *German Law Journal* 522.

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 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.

CHAPTER V

CYBER CRIMES

5.1 Individual Responsibility for War Crimes Committed in Cyberspace under Domestic Criminal Law and International Criminal Law

By ***Robert Łasa*** (University of Silesia)

Introduction

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 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.

The paper is divided into two parts. The first one presents the genesis of individual criminal responsibility for war crimes and defines a war crime. In addition, the first part describes the criminal responsibility of an individual for crimes committed in cyberspace from the perspective of international law. The second part is a review of national war crimes regulations of selected countries - the United States of America (USA), the United Kingdom (UK), the People's Republic of China (China), and the Russian Federation (Russia). 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.[571] 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 (ICC Statute). The first three states are not parties to the ICC Statute, whereas the UK ratified it in 2001.

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

[571] 'Iran, Victim of Cyber warfare' (*ICRC Casebook*) <https://casebook.icrc.org/case-study/iran-victim-cyber-warfare> accessed 30 October 2023.

theoretical method, which indicates the position of doctrine and the content of legally non-binding documents.

1. War crimes: introduction

The development of legal procedures to bring an individual to responsibility for war crimes has been a long and often complicated process. The landmark in the development of responsibility for war crimes was the period after World War II (WW II) when the victorious powers concluded the Agreement for the Prosecution and Punishment of the Major War Criminals of the European Axis, and Charter of the International Military Tribunal (IMT Charter).[572] The Agreement established the International Military Tribunal in Nuremberg (IMT) to prosecute the worst Nazi criminals for crimes against peace, war crimes, and crimes against humanity.[573] The IMT Charter defined war crimes as violations of the laws and customs of war, then listing them by example, such as murder and deportation for forced labor (see Article 6(b) of the IMT Charter).

Another important period for the development of responsibility for war crimes was the 1990s. The experience of two bloody armed conflicts (in Rwanda and the former Yugoslavia) led to the establishment of international criminal tribunals to prosecute those responsible for crimes committed during these conflicts.[574]

The International Criminal Tribunal for the former Yugoslavia (ICTY) did not include a "single, collective" war crime in its statute. Still, it referred to grave breaches of the Geneva Conventions of 1949 and violations of the laws and customs of war.[575] The former has a closed catalog, including willful killing, torture, or inhuman treatment (see Article 2 of the ICTY Statute). Violations of the laws and customs of war are not limited but only listed by way of examples, such as employment of poisonous weapons or other weapons calculated to cause unnecessary suffering (see Article 3 of the ICTY Statute).

Five years after establishing the ICTY, the Statute of the ICC was signed.[576] It is the first permanent international criminal court in history to try genocide, crimes against humanity, war crimes, and crime of aggression.

1.1 War crimes: definition

The ICC Statute defined war crimes as grave breaches of the 1949 Geneva Conventions by enumerating, for example wilful killing, wilfully causing great suffering, or serious injury to body or health (see Article 8(2)(a) of the ICC Statute), but also other serious violations of the laws and customs applicable in armed conflict (see Article 8(2)(b) and 8(2)(e) of the ICC Statute). The latter finds its application both in an armed conflict of an international character (IAC) and an armed conflict of

[572] Agreement for the Prosecution and Punishment of the Major War Criminals of the European Axis, and Charter of the International Military Tribunal, 8 August 1945, 82 UNTS 251.

[573] Cassese A, Acquaviva G, Fan M, Whiting A, *International Criminal Law: Cases & Commentary* (OUP, 2013), pp. 27–29.

[574] Bassiouni MC, *Introduction to International Criminal Law* (2nd edn. Martinus Nijhoff, 2013), p. 1070.

[575] UNSC, Res. 827 'Statue of the International Criminal Tribunal for the Former Yugoslavia', annex, UN Doc. S/RES/827 (1993).

[576] Statute of the International Criminal Court, 17 July 1998, 2187 UNTS 90.

a non-international character (NIAC). Serious violations of common Article 3 to the 1949 Geneva Conventions, which are listed as a closed catalog, e.g., violence to life and person, in particular murder of all kinds, mutilation, cruel treatment and torture, should also be considered war crimes (see Article 8(2)(c) of the ICC Statute).

Besides the legal definition found in the ICC Statute, special attention should be given to additional grounds described in the jurisprudence of international criminal tribunals. An example of this is the so-called *Tadić test*, which was cited in the case of the President of the Local Board of the Serb Democratic Party.[577] According to this, four conditions must exist to establish war crimes: the violation must constitute an infringement of a rule of international humanitarian law, the rule must be customary in nature or, if it belongs to treaty law, the required conditions must be met, the violation must be "serious", that is to say, it must constitute a breach of a rule protecting important values, and the breach must involve grave consequences for the victim, the violation of the rule must entail, under customary or conventional law, the individual criminal responsibility of the person breaching the rule.[578]

An important factor is to link the war crime to the armed conflict taking place. The purpose of this is to distinguish "ordinary" crimes from crimes committed in the context of an armed conflict. This was pointed out by the ICTY, which stated that the place where the crime was committed was irrelevant, the mere fact that it was connected with an armed conflict taking place on the whole territory of a given state (IAC) or over the entire territory under the control of a party to the conflict (NIAC) was sufficient.[579]

1.2 War crimes in cyberspace

To date, neither national courts nor international tribunals have tried those responsible for war crimes committed in cyberspace. Of course, this does not mean that such crimes cannot occur in the future. Neither the countries' domestic law cited in the text nor international law directly regulates criminal activity in cyberspace. Still, by applying an analogy from the ICC Statute, several possibilities for such crimes can be envisaged. Three possibilities of committing war crimes in cyberspace will be presented below. It should be noted that the catalog presented is illustrative, and there may be more possibilities.

The first example is an attack aimed directly at the civilian population, primarily individuals civilian. Adversary forces using malware can attack hospitals by modifying critical information in patient records.[580] By modifying a patient's medical information, a doctor could make the wrong treatment decision, thus leading to the patient's death. Such action violates Article 51(2) of Additional Protocol I to the 1949 Geneva

[577] 'Case Information Sheet: Duško Tadić' <https://www.icty.org/x/cases/tadic/cis/en/cis_tadic_en.pdf> accessed 30 October 2023.

[578] ICTY, *Prosecutor v. D. Tadić, Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction*, IT-94-1 (2 October 1995).

[579] ICTY, *Prosecutor v. Kunarac et al., Appeals Chamber Judgement,* IT-96-23 & IT-96-23/1-A (12 June 2002), para 57.

[580] Schmitt M, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (CUP, 2017), p. 423.

Conventions (AP I)[581] and Article 13(2) of Additional Protocol II to the 1949 Geneva Conventions (AP II).[582] Those responsible for modifying relevant data in a patient's file would be responsible for intentionally directing attacks against the civilian population as such or against individual civilians not taking direct part in hostilities (see Article 8 (2)(b)(i) and Article 8 (2)(e)(i) of the ICC Statute).

The second example is the intentionally launching an attack in the knowledge that such attack will cause incidental loss of life or injury to civilians or damage to civilian objects or widespread, long-term and severe damage to the natural environment which would be clearly excessive in relation to the concrete and direct overall military advantage anticipated (see Article 8 (2)(b)(iv) of the ICC Statute). A cyberattack targeting a nuclear power plant or other nuclear facilities could cause civilian harm and environmental damage. This is due to the radiation released into the atmosphere when a facility caused by a cyberattack explodes. IHL prohibits attacking facilities that contain dangerous forces (see Article 56 of PD I and Article 15 of PD II).

The last example is an attack directed at buildings dedicated to religion, education, art, science or charitable purposes, historic monuments, hospitals and places where the sick and wounded are collected, provided they are not military objectives (see Articles 8(2)(b)(ix) and 8(2)(e)(iv) of the ICC Statute). An attack targeting a hospital that could cause civilian deaths has already been described above. Obviously, there is the possibility of a cyberattack that would disable the hospital as a whole. Such a situation occurred in March 2020 when an unknown group of hackers attacked a hospital in Brno (Czech Republic), preventing aid to people infected with the SARS-CoV-2 virus.[583] Conducting such an attack during and connected with an armed conflict would establish a war crime.

1.3 Individual criminal responsibility

The commission of a war crime gives criminal responsibility to the individual. Anyone who commits the crime itself, but also anyone who ordered the commission of the crime, assisted in the commission of the crime, or in any other way contributes to the commission of the crime is responsible for the serious violations set out in the ICC Statute (see Article 25(3) of the ICC Statute). A necessary element of an individual's criminal responsibility is the intent to commit the crime. The person committing it knows that he is committing a war crime within the meaning of the ICC Statute (*mens rea*, see Article 30 of the ICC Statute). The vast majority of offenses are committed with *dolus directus*, but some of the elements of the criminal act will also be fulfilled with *dolus eventualis* or through recklessness.[584]

---

[581] Additional Protocol to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts, 8 June 1977, 1125 UNTS 3.

[582] Additional Protocol to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non-International Armed Conflicts, 8 June 1977, 2404 UNTS 609.

[583] 'Brno University Hospital ransomware attack' (2020) <https://cyberlaw.ccdcoe.org/wiki/Brno_University_Hospital_ransomware_attack_(2020)> accessed 30 October 2023.

[584] Schmitt M, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (CUP, 2017), p. 392.

The ICL also provides criminal responsibility for the commander and other superiors. The ICC Statute identifies three situations in which the commander's responsibility will arise: when he orders the conduct of an operation that fulfills elements of a war crime, when he knew or, owing to the circumstances at the time, should have known that the forces were committing or about to commit such crimes, or when he failed to take all necessary and reasonable measures within his power to prevent or repress their commission or to submit the matter to the competent authorities for investigation and prosecution (see Article 28 of the ICC Statute).

Nowadays, most world powers have cyber army units, e.g., U.S. Cyber Command (USA) or the Russian military intelligence service GRU (Unit 74455). In such a case, identifying the soldier responsible for committing a cyberwar crime and his commander should not raise a problem, provided that the state of the armed forces is willing to prosecute them. Law enforcement faces a much greater challenge when civilians, known as hackers, commit war crimes. Often these are informal groups of civilians cooperating with special services, remaining fully anonymous, such as the Russian Business Network (RBN).[585] The inability to identify hackers limits their prosecution for war crimes.

2. War crimes in domestic law

The seriousness of war crimes has led the international community to create a system that would ensure the efficient trial of those who commit such acts. The creation of the ICC follows the steps taken to organize this system. However, the ICC Statute itself prioritizes national courts in conducting criminal proceedings against war crimes perpetrators (see Article 1 of the ICC Statute). This approach entails the creation of national regulations to enable the prosecution and subsequent trial of war criminals.

2.1 War crimes in American law

America's war crimes legislation came first in 1996 when President Bill Clinton signed the War Crimes Act 1996.[586] The Act was amended three times over the next ten years, with the most significant amendment introduced by the Military Commissions Act 2006.[587]

A member of the US armed forces or a US citizen who has committed a war crime may be prosecuted. Under the definition set forth in the Act, a war crime is a grave breach in any of the international conventions signed at Geneva 12 August 1949, or any protocol to such convention to which the United States is a party (it should be noted that the US is not a party to the PD I and PD II), violation of prohibition by Article 23, 25, 27, or 28 of the Annex to the Hague Convention IV, Respecting the Laws and Customs of War on Land, signed 18 October 1907 (1907 Hague Regulations)[588],

[585] Rzeszuta M, 'Sieć. Piąty Teatr Działań Wojennych: 2008 – Informatyczna Blokada Gruzji' (2020) *Układ Sił* 23, p. 52.

[586] '18 U.S. Code § 2441 – War crimes' (*Cornell Law School*) <https://www.law.cornell.edu/uscode/text/18/2441> accessed 30 October 2023.

[587] *Military Commissions Act 2006 (c 5) USPL 109-366* (2006).

[588] Convention (IV) Respecting the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land, 18 October 1907, 36 Stat. 2277.

a grave breach of common Article 3 to the 1949 Geneva Conventions, and willfully killing or causing serious injury to civilians, what violates the Protocol on Prohibitions or Restrictions on the Use of Mines, Booby-Traps and Other Devices as amended at Geneva on 3 May 1996 (see 18 US Code § 2441(b))[589].

Despite a transparent system for prosecuting and trying war criminals, the USA is not willing to do so, at least in the context of its citizens. Committing a war crime in cyberspace is one of the main reasons for the inability to find the person responsible for such acts. Nowadays, technology offers great opportunities to remain anonymous online, which is often exploited by official and unofficial hacker groups (concerning cyber armies and "common" hackers). An additional complication is the concealment of criminals by their state authorities. Unfortunately, in the case of the USA, a large number of war crimes committed by US soldiers in Afghanistan were concealed, or even, in the case of evidence confirming the commission of war crimes, those responsible were not held accountable[590]. This is particularly evident in the conflict between the USA and the ICC. Although the US government actively participated in the negotiations on the ICC Statute, it is not a party to this international agreement[591]. The conflict culminated in 2020 when the ICC agreed to commence an investigation into alleged crimes under the jurisdiction of the Court in relation to the situation in Afghanistan[592]. The investigation was supposed to include the activities of US armed forces in the country from 2003 to 2004. The US response was to impose sanctions on individuals connected with the ICC. President Donald Trump issued legislation blocking the property of certain persons associated with the ICC[593]. In addition to economic sanctions, individuals involved in the work of the Court (e.g., lawyers, judges) could be banned from entering US territory.

The reluctance to prosecute war criminals or those who otherwise violate international law who are members of the U.S. armed forces or citizens of this country does not correlate to prosecuting citizens of other countries who commit such acts. An example of this is the indictment of GRU soldiers who, known as SandWorm, committed cyberattacks on Ukrainian energy infrastructure in 2015 and 2016.[594]

---

589 Protocol on Prohibitions or Restrictions on the Use of Mines, Booby-Traps and Other Devices, 3 May 1996, 2048 UNTS 93.

590 Ning YB, 'How US Evades Responsibility for War Crimes in Afghanistan' (*Global Times*, 27 September 2021) <https://www.globaltimes.cn/page/202109/1235240.shtml?id=11> accessed 30 October 2023.

591 Amann DM, Sellers MNS, 'The United States of America and the International Criminal Court' (2002) 50 *The American Journal of Comparative Law* 381, pp. 381-383.

592 ICC *Judgment on the appeal against the decision on the authorisation of an investigation into the situation in the Islamic Republic of Afghanistan*, Judgment [2020] ICC-02/17-138.

593 Blocking Property of Certain Persons Associated with the International Criminal Court, 11 June 2020, Executive Order 13928.

594 'Six Russian GRU officers charged in connection with worldwide deployment of destructive malware and other disruptive actions in cyberspace' (*United States District Court Western District of Pennsylvania*, 19 October 2020) <https://www.justice.gov/usao-wdpa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware> accessed 30 October 2023.

2.2 War crimes in Britsh law

As one of the victorious states of WW II, the UK took an active part in trying war criminals. This undoubtedly contributed to the subsequent development of national criminal law concerning serious violations of IHL. Less than ten years after the Nuremberg trials, the UK authorities decided to regulate the punishment of crimes committed during armed conflict.[595] The act introduced criminal responsibility for individuals committing grave breaches of the 1949 Geneva Conventions and AP I. In addition, responsibility for grave breaches of PD III was incorporated into the national criminal system by the 2009 amendment. The regulation applies to any person, whatever his nationality, who in the UK or any other country commits, aids, or abets this crime (see Chapter 52(1) Geneva Conventions Act 1957).

In October 2001 UK ratified the ICC Statute.[596] A few months earlier, the British government had prepared national legislation under which the UK recognizes genocide, crimes against humanity, and war crimes under the ICC Statute.[597]

A few years later, the British justice system faced the trial of war criminals. According to NGO reports and witness testimony, British armed forces allegedly committed serious violations of international law during the intervention in Iraq between 2003 and 2009[598]. In 2006, a soldier was convicted of inhuman treatment (beating a prisoner who died as a result)[599]. He was the only person convicted of war crimes committed in Iraq by British armed forces. Later, a special team was established to investigate violations of international law during the British intervention in Iraq (mainly inhumane treatment of prisoners held in British prisons).[600] The Iraq Historic Allegations Team (IHAT) operated for seven years, from 2010 to 2017, without leading to the prosecution of any soldier who remained suspected of having committed a war crime.[601]

The activity of prosecution bodies to explain the alleged war crimes committed by British soldiers in Iraq between 2003 and 2006 indicates a reluctance to bring to justice those soldiers who committed the crimes. Despite the intensive work of the aforementioned bodies, only one person has been convicted, while NGO reports and witness testimonies have pointed to more soldiers involved in violations of international

---

595 Geneva Conventions Act 1957, 31 July 1957, UK Public General Acts 1957 c. 52.

596 The States Parties to the Rome Statute: United Kingdom, <https://asp.icc-cpi.int/en_menus/asp/states%20parties/western%20european%20and%20other%20states/Pages/united%20kingdom.aspx> accessed 30 October 2023.

597 *International Criminal Court Act c. 17*, UK (2001).

598 Human Rights Watch, 'Pressure Point: The ICC's Impact on National Justice' (*HRW*, 3 May 2018) <https://www.hrw.org/report/2018/05/03/pressure-point-iccs-impact-national-justice/lessons-colombia-georgia-guinea-and#_ftn576> accessed 30 October 2023.

599 'British soldier admits war crime' (*BBC News*, 30 October 2023) <http://news.bbc.co.uk/2/hi/uk_news/5360432.stm> accessed 30 October 2023.

600 'Iraq Historic Allegations Team (IHAT)' (*Gov.UK*) <https://www.gov.uk/government/groups/iraq-historic-allegations-team-ihat> accessed 30 October 2023.

601 'The Iraq Historic Allegations Team (IHAT) Quarterly Update' *(The Iraq Historic Allegations Team*, 20 July 2017) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/644256/20170809-Quarterly_Update_website_Jun17_1_.pdf> accessed 30 October 2023, pp. 2-3.

law. This approach of national justice bodies is an obstacle to fulfilling their obligations under international agreements to prosecute war criminals.

Another threat in trying war criminals operating in cyberspace is remaining anonymous online. This problem has already been described in the case of the American legal system (see page 8).

2.3 War crimes in Chinese law

China's criminal law lacks provisions on the criminalization of war crimes.[602] The doctrine suggests that the only way to hold war criminals criminally responsible for their actions is to use an analogy from other provisions that criminalize specific conduct, such as Article 232 of the Chinese Penal Code (homicide).[603]

The lack of appropriate national regulation, together with the non-ratification of the ICC Statute, constitutes a serious threat to the trial of those responsible for war crimes. It should be noted that most of the crimes that can be committed in cyberspace are carried out by hacker groups unofficially connected with governments (e.g., the RBN, which committed cyber attacks for the benefit of Russia, during the armed conflict in Georgia in 2008).[604]

As China has not ratified the ICC Statute, the only way to exercise ICC jurisdiction over crimes committed by Chinese nationals is for the United Nations Security Council (UNSC) to refer the case to the ICC Prosecutor under Article 13 of the ICC Statute. It should be noted here that China is a permanent member of the UNSC, and its veto will stop the above-mentioned procedure. Thus, war criminals will go unpunished under domestic law, and the ICC will not be able to proceed against them.

2.4 War crimes in Russian law

The issue of war crimes in the Russian legal system was first addressed in 1965 when the Decree on Punishment of War Criminals was issued.[605] Its provisions applied to all nations of the Soviet Union that suffered during WW II. Accordingly, those who committed war crimes during WW II were subject to prosecution and punishment. Currently, the punishability of war crimes is derived from the 1996 Criminal Code.[606] It regulates criminal responsibility for cruel treatment of prisoners of war, deportation of civilians, the pillage of national property on occupied territory, and use in armed conflict of means and methods of warfare prohibited by international treaties to which Russia is a party.

Despite the appropriate regulation of criminal responsibility of war criminals, Russia does not prosecute its citizens based on these laws. There have been numerous

---

602 *Criminal Law of the People's Republic of China,* PRC (1997).

603 Deng H, 'What can China do to develop International Criminal Law and Justice further from the perspective of the International Criminal Court?' (2016) 5 *Revista Tribuna Internacional* 9, p. 26.

604 Swanson L, 'The Era of Cyber Warfare: Applying International Humanitarian Law to the 2008 Russian-Georgian Cyber Conflict' (2010) 32 *Loyola of Los Angeles International and Comparative Law Review* 303.

605 *Practice Relating to Rule 158. Prosecution of War* Crimes <https://ihl-databases.icrc.org/customary-ihl/eng/docs/v2_rul_rule158> accessed 30 October 2023.

606 *Criminal Code of The Russian Federation No. 63-Fz of 13 June 1996,* Russian Federation (1966).

violations of international law by Russian citizens in cyberspace in the context of armed conflict, and they have not been tried for it. This is mainly the case of attacks in cyberspace during the armed conflicts in Georgia (2008) and Ukraine (2015-2016) described above.

It also appears impossible to initiate investigations before the ICC. First of all, Russia has not ratified the ICC Statute. Moreover, as a permanent member of the UNSC, it can veto the procedure set out in Article 13 of the ICC Statute.

Conclusion

The progressive development of technology makes it possible to conduct armed conflict at a distance, even several thousand kilometers from the actual battlefield, all by using a computer. Conducting combat in cyberspace has pros and cons. On the one hand, it makes it possible to limit losses among combatants. Still, on the other hand, it makes it possible to remain fully anonymous, or at least to remain anonymous for a very long time. This creates a certain sense of impunity, making it relatively easy for soldiers or civilians who commit cyberattacks to cross the boundary drawn by IHL and commit war crimes.

Unfortunately, the world powers, leading the way in developing military capabilities in cyberspace, may not be interested in prosecuting war criminals from cyberspace, just as they did not do so with war criminals from Iraq or Afghanistan (USA, UK) or do not have appropriate regulations in their legal system to allow such prosecutions (China). This would leave war criminals unprosecuted.

5.2 The Limits to the Use of Force in Cyberspace: The Tallinn Manual Perspective

By ***Marek Gerle and Adam Crhák*** (Charles University)

Introduction

The concept of the use of force has represented one of the cornerstones of modern international law and served as the base of the post-WWII security architecture for more than seven decades now. The contemporary *ius ad bellum,* petrified by the UN Charter and later elaborated in different ICJ cases, stands as a solid body of law regulating the resort to force in international relations. But what if the reality of the 21st century surpassed the traditional concept and new cyber means of warfare were employed?

The 2007 cyber-attacks on Estonia and the Russo-Georgian war a year later reinvigorated the focus of international legal scholarship on this peculiar subject. The Tallinn Manual, as well as its version 2.0 (and soon-to-come 3.0), came into existence due to the newly felt urgency of the upgraded shape of modern warfare. To this day, the project represents the most comprehensive attempt to depict the current state of normativity regulating the use of force with regards to cyberspace. Ever since the publication of its first volume, the Manual has elicited a considerable number of various reactions from concurrent legal scholars and States representatives alike.

The aim of this article is to present an analysis of its stance towards the use of force in the digital sphere as well as the reactions and evaluations from relevant stakeholders. The ultimate objective is to shed light on the normative quality of the Manual and its potential of becoming an expression of binding principles and rules of the prospective international law. Has the Manual become too influential to be disregarded in relation to the future conception and codification of normativity of the *ius ad bellum* in cyberspace?

Due to the limitations of the given format, the paper will concentrate on the notions of the use of force, armed attack and the possible attribution of the given acts. Questions of the collective form of self-defense and actions under the Chapter VII of the UN Charter will not be dealt with in detail.

1. The use of force in cyberspace

As in other fields of the law, the inherent abstractness of normativity concerning the use of force does not prevent the regulation from advancing, yet on the contrary it allows it to develop regarding new challenges. In its far-reaching advisory opinion on the *Legality of Nuclear Weapons*, the ICJ observed that the relevant provisions of the UN Charter applied to any use of force, regardless of the weapons employed.[607] In conformity with this stance, even the cutting-edge cyber-technologies, when used in an equivalent manner as traditional weapons, could fall under the legal regime of the art. 2 (4) of the

[607] ICJ, *Legality of the Threat of Use of Nuclear Wapons, Advisory Opinion* [1996] ICJ Rep 1996, para 39.

Charter. This prerequisite later allowed for a new dimension of the cyber law to develop as well as for the inception of the original Tallinn Manual itself.

However, the reality is multifarious, and not every utilization of cyber means constitutes a breach of the *ius ad bellum*. The threshold of what is considered a use of force in international law, coined in the previous decades, should apply to contemporary conditions. Quite famously recorded in the *travaux préparatoires*, the architects of the UN Charter did not want it to include economic coercion,[608] which was also confirmed and affiliated with sorts of political duress and pressure in the Declaration on Friendly Relations adopted by the UN General Assembly a quarter of a century later.[609] On the other hand, the prohibition of the recourse to force in Art. 2 (4) of the Charter proscribes any threat or use of force in any other manner inconsistent with the Purposes of the United Nations.[610] Once again, the supposed original meaning behind this formulation is evidenced by the *travaux préparatoires* as overlapping any threat or use of force not falling within the categories of territorial integrity or political independence of (UN member) States.[611] The applicability of the widely recognized exceptions to the prohibition will be dealt with later in the article.

Although there is no general authoritative definition of what constitutes a threat and use of force, the international community benefits from some of the criteria of illegal use of force and armed attacks articulated by the ICJ in the notorious *Nicaragua* case. For instance, the Court decided that mere funding of guerillas engaged in armed hostilities, otherwise unattributable to the assisting State, or mere frontier incidents, do not amount to the use of force. Contrarily, providing training and arms to the guerillas in fact does involve the threat or use of force against the injured State.[612]

How do these requirements translate to the modern dimension of cyber warfare? The International Group of Experts (IGE) behind the Tallinn Manuals resolutely agreed on the fact that "*there is no basis for excluding cyberoperations from within the scope of actions that may constitute a use of force if the scale and effects of the operation in question are comparable to those of non cyber operations that would qualify as such*."[613]

---

608 6 UNCIO. Docs. 334, 609 (1945); Doc. 2, 617 (e) (4), 3 UNCIO. Docs. 251, 253-54 (1945).

609 UNGA, 'Declaration on Principles of International Law concerning Friendly Relations and Cooperation among States in accordance with the Charter of the United Nations', UN Doc. A/RES/2625(XXV) (1970).

610 UN, Charter of the United Nations, adopted on 24 October 1945, 1 UNTS 16, Art. 2, para 4.

611 See, travaux péparatoires (n 608).

612 ICJ, *Case Concerning Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America)*, Judgment [1986] ICJ Rep 392, para 228.

613 Schmitt M, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (CUP, 2017), p. 331, and similarly in:
Schmitt M, *Tallinn Manual on the International Law Applicable to Cyber Warfare* (CUP, 2013), p. 19.
Confirmed also by the reports by the following UN GGE reports:
UNGA, 'Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security', UN Doc. A/68/98, para 19 (June 24, 2013);
UNGA, 'Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security', UN Doc. A/70/174, para 24 (July 22, 2015);
Roscini M, 'World wide warfare: Jus ad bellum and the use of cyber force' (2010) 14 *Max Planck YBUNL* 85, p. 106.

Following up on the example of assistance to guerillas and other groups distinguished from the State in question, this may easily be performed with a striking resemblance in the cyber context. Providing groups of so-called hacktivists with malware, ransomware, etc. and/or training them in the usage against an enemy State would *per analogiam* constitute an infringement of the prohibition by the assisting State. Needless to say, that the mere financing of such groups without any other significant contribution would not amount to such a violation.[614]

Taking a step back to the issue of qualification of situations acknowledgeable as the use of force in international law, there are some conditions set by the ICJ in its previous case law, that could serve as an instructive guideline. For the determination of an armed attack, another crucial term of art setting the required threshold in the modern self-defense regulation, in *Nicaragua* the ICJ again made use of the Declaration on Friendly Relations and differentiated the most grave forms of the use of force constituting an armed attack from other less grave forms.[615]

This position was subsequently refused by the United States, which articulated a position, later embraced by some parts of the scholarship, opposing any discretion between the levels of use of force and armed attacks.[616] Nevertheless, the preponderant part of the international community stands behind the distinctive conception, that leads to a simple conclusion of *a minori ad maius* – any armed attack constitutes the use of force, whereas the use of force does not qualify as an armed attack does not have any universal definition within the case law, binding normative documents or customary international law.[617] Although not being precisely defined, the distinction bears an important value in prescribing the boundary between a lawful reaction involving the recourse to force in self-defense to an armed attack in comparison to a reaction not involving any use of force to a less-intensity use of force by the initiator.

At this point, the Tallinn Manual comes with a proposition of a set of eight suggested factors derived from an earlier original conception by its editor and the leading figure of the Tallinn process, prof. Michael Schmitt.[618] The following criteria are claimed to be designed to identify cyber operations correspondent to acts traditionally qualifiable as use of force, kinetic or non-kinetic in its nature.[619] The factors, as a progressive element

[614] Schmitt M, *Tallinn Manual on the International Law Applicable to Cyber Warfare* (CUP, 2013), p. 48; Schmitt M, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (CUP, 2017), p. 332.

[615] ICJ, *Case Concerning Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America)*, Judgment [1986] ICJ Rep 1986, para 191.

[616] United States Department of Defence Law Manual (June 2015, Updated July 2023), pp. 47–48, para 1.11.5.2.
Based inter alia on: Sofaer AD, 'The Sixth Annual Waldemar A. Solf Lecture in International Law: Terrorism, the Law, and the National Defense' (1989) 126 *Mil L Rev* 89, pp. 92-93 (1989); Taft WH IV, 'Self-Defense and the Oil Platforms Decision' (2004) 29 *Yale J Int'l L* 295, pp. 300–301 (2004).

[617] See e.g., Focarelli C, 'Self-Defence in Cyberspace' in *Research Handbook on International Law and Cyberspace* (Elgar, 2021), p. 328 and following.

[618] Schmitt M, 'Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework' (1999) 37 *Colum J Transnat'l L* 885, p. 914.

[619] Schmitt M, *Tallinn Manual on the International Law Applicable to Cyber Warfare* (CUP, 2013), p. 49 and following; Schmitt M, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (CUP, 2017), p. 334 and following.

in the discourse, deserve a closer commentary and an analysis of the up-to-date scholarly discussion.

Firstly, the *Severity* of the cyber operation is presented as the most significant factor in any such analysis. Working on the presumption that consequences of the operation in question will involve some degree of physical harm to individuals and/or property, the scope, duration, and intensity of the consequences are assumed to be influential aspects in the qualification.

Secondly, the *Immediacy* of the manifestation of consequences is alleged to be of considerable importance *vis-à-vis* the hypothetical reaction, meaning that operations with repercussions deferred or distributed in time are less unlikely to be perceived and countered in a peaceful manner.

The *Directness* of interlinkage between the initial act and its consequences is proclaimed to indicate a more transparent causal connection eventuating into a recognition of the act as a case of illegal use of force.

The aspect of *Invasiveness* concerns the level of intrusion into a cyber system in connection to its constitution and protection against any such external interference. Intrusion into highly protected military cyber systems appears to be more disturbing than to any ordinary vulnerable system of a SME or a public institution.

As consequences of cyber operations are frequently hard to quantify, the possible *Measurability of effects*, allowing for a more precise identification of an impact of the operation on a scale appropriate for such technical matters, is considered to simplify postulating of an attainment of the level of the use of force.

The traditional conception of the UN Charter and its focus on armed force led the authors of the Tallinn Manual to emphasize the *Military character* of the cyber operations as one of the factors significantly affecting its evaluation and classification as unlawful use of force. A potential connection between any such operation and other conventional military actions should serve as a solid signal. Similarly, the degree of *State involvement*, military or not, direct or indirect, may indicate the plausibility of an infringement by that State of the cogent prohibition of the use of force in international law.

The last factor of *Presumptive legality* appears to tend to balance the potentially expansive interpretation of cyber force towards the threshold of the use of force. The illustrious Lotus principle, stating that by the fundamentally permissive nature of international law sovereign States may act at their discretion, unless for finding themselves restricted by an explicit prohibition,[620] is indirectly alluded to by the Tallinn Manual.

Besides the presented categories, the authors of the Manual recognize the importance of other factors, such as of the predominant political environment, foreseeable further military operations, the nature of the target, and the profile and previous record of the offender.[621]

---

[620] *PCIJ, S.S. Lotus (France v. Turkey) Judgment [1927] PCIJ (Ser. A) No. 10, 18,* p. 18.

[621] Schmitt M, *Tallinn Manual on the International Law Applicable to Cyber Warfare* (CUP, 2013), pp. 49–52; Schmitt M, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (CUP, 2017), pp. 333–337.

Several States have expressed their positions on this matter. The Netherlands explicitly endorsed the approach of the Manual.[622] The United States lists, among other criteria, the context of the event, the actor perpetrating the action (bearing in mind possible obfuscation techniques), the target and its location, the effects of the cyber activity, and the intent of the actor.[623] In Germany's non-exhaustive list of criteria, it is the severity of the interference, the immediacy of its effects, the degree of intrusion into a foreign cyber infrastructure, and the degree of organization and coordination of the malicious cyber operation, which may play a significant role in the assessment.[624] Estonia, probably in light of the 2007 DDoS attacks, considers the requisites for qualification of use of force to include operations targeting critical infrastructure, yet necessarily resulting in serious damage, injury or death.[625] What is to be principally agreeable with, is the observation that any such factors should be reflected in concordance to reach an optimal conclusion over the complex matter in question.

Decoding the postulated legal regime of the recourse to force in international law in a cyber context, one must not forget to draw attention to the possibly antecedent acts of threat of force. The cyber dimension of this subject may materialize either in a threat of a forceful cyber operation or a cyber threat of the use of force in a kinetic or non-kinetic manner. The conditions seem otherwise similar to the threats against States in a traditional legal setup.

Last but not least, any cyber operations not reaching the threshold of the use of force may however be considered as contravening other rules of the international law. Those include the principle of non-intervention in the internal affairs of States[626] going hand in hand with the obligation to respect the sovereignty of States and possible other obligations.

2. Self-defense in the cyber context

The concept of self-defense, as one of the two major exceptions of the peremptory prohibition of the use of force in modern international law, represents a fundamental keystone of contemporary security architecture. Emanating from the archaic conception of *bellum iustum*, the right of self-defense against alien force most certainly persists as a crucial element even in the hi-tech cyber era.

---

[622] 'Letter to the parliament on the international legal order in cyberspace' (*Government of the Netherlands*, July 2019) <https://www.government.nl/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace>, p. 4.

[623] UNGA, 'United states of America: Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States submitted by participating governmental experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security established pursuant to General Assembly resolution 73/266', (2021) <https://front.un-arm.org/wp-content/uploads/2021/08/A-76-136-EN.pdf.>, p. 137.

[624] 'On the Application of International Law in Cyberspace, Position paper' (*The Federal Government of Germany*, March 2021), <https://www.auswaertiges-amt.de/blob/2446304/2ae17233b62966a4b7f16d50ca3c6802/on-the-application-ofinternational-law-in-cyberspace-data.pdf>, p. 6.

[625] UNODA, 'Estonia: Official compendium of voluntary national contributions', A/76/136, (2021), p. 26.

[626] UN Charter, Art. 2 (7).

Art. 51 of the UN Charter, in reference to the customary right of individual and collective self-defense, petrifies its universal and natural (inherent) form while conditioning the contours of its possible application.[627] The aforementioned notion of an armed attack, notably interpreted in the *Nicaragua* case, stands as a key precondition to any such reaction involving the use of force by the attacked State. The ICJ drew a line between the use of force, as a larger aggregate of forceful acts, and those amounting to armed attacks justifying the otherwise proscribed use of force in response.[628]

In regard to the noticeable attribute of the attack, that describes it as armed, the Tallinn Manual repeatedly alludes to the advisory opinion on *Nuclear weapons* where the ICJ negates any attachment toward the character of the weapons used.[629] The effects of e.g. biological or chemical weapons without any considerable material destruction are proclaimed comparable to the effects of attacks in the cyber domain. Moreover, as the final assessment concerning this issue, by comparison of the impact of cyber-operations, inflicting analogous effects as their kinetic counterparts, the armed attacks do not necessarily, in the eyes of the authors of the Tallinn Manual, require any such employment of weapons of any kind.[630]

Regarding the necessary degree of force employed to attain the threshold of the armed attack, the ICJ restrained itself only to presenting such acts as the gravest forms of the use of force.[631] The Tallinn Manual demonstrates this notional category of such acts in the cyber domain as equivalents to physical acts engendering deaths and injuries of individuals, as well as damages and destructions of property. Conversely, the actions non amounting to armed attacks are illustrated by acts of cyber-theft, gathering of cyber-intelligence, or minor interruptions of non-essential cyber-infrastructure.[632]

The eventuality of a multitude of lesser individual incidents, bonded altogether to a composite attack, poses a question of whether those acts may constitute such serious infringement of the prohibition of force aggregating to the intensity of an armed attack. The Tallinn Manual (in concord with the pin-prick doctrine)[633] answers this question in the positive. The interconnection between such acts with identical or concerted actors

---

627 UN Charter, Art. 51.

628 ICJ, *Case Concerning Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America)*, Judgment [1986] ICJ Rep 1986, para 191 and following; ICJ, *Case Concerning Oil Platforms (Islamic Republic of Iran v. United States)*, Judgment [1996] ICJ Rep 2003, paras 161, 183, 196–8.

629 ICJ, *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion [1996] ICJ Rep 1996, para 39.

630 Schmitt M, *Tallinn Manual on the International Law Applicable to Cyber Warfare* (CUP, 2013), p. 54; Schmitt M, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (CUP, 2017), p. 340.

631 ICJ, *Case Concerning Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America)*, Judgment [1986] ICJ Rep 1986, para 191.

632 Schmitt M, *Tallinn Manual on the International Law Applicable to Cyber Warfare* (CUP, 2013), p. 55; Schmitt M, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (CUP, 2017), p. 341.

633 See e.g., Abhimanyu GJ, Rationalising International Law Rules on Self-Defence: The Pin-Prick Doctrine (June 26, 2014). XII(2) *Chicago-Kent Journal of International and Comparative Law* 23 (2014).

was recognized as the key qualificators for meeting the threshold with the required effects and scale.[634]

Conversely, in regard to operations not resulting in any physical damage, the authors of the Manual did not take a common stance. However severe the consequences of such attacks might otherwise be, the fact that no physical destruction, injury or death are engendered, divides the scholarship in this question. Using the popular example of the collapsed Stock Exchange, such "non-violent" attacks might lead to serious disturbance impacting the whole economy of the targeted State (not to even mention the potential transnational dimension) with grave financial damages. This scenario might seem to some as graver than others involving minor physical damages or destruction. Nevertheless, until now there is no general agreement over the character and legal qualification of such acts.

In connection to the possibility of cyber-operation without physical damage being acknowledged as use of force, France presented a list of factors and circumstances prevailing at the time of the operation, such as the origin of the operation and the nature of the instigator (military or not), the extent of intrusion, the actual or intended effects of the operation or the nature of the intended target.[635] The Netherlands did not want to *a priori* rule out such operations having a very serious negative financial or economic impact.[636] Similarly, Norway considers operations engendering widespread economic destabilization as potentially amounting to the use of force in violation of Article 2 (4).[637] Italy leaves the door open for potential recognition of non-physical damage attacks due to the modern world's reliance on digital technologies which may lead to the interruption of essential services without the need for physical damage.[638]

Moving on to the phase of a forceful reaction to the armed attacks, the question of necessity and proportionality arises as a crucial limitation to this exceptional recourse to force in international law. As in the traditional conception, the effectuation of the right to defend oneself in the cyber environment is required to fulfill the criteria confirmed many times by international judicial institutions and considered customary.[639] The

---

634 Schmitt M, *Tallinn Manual on the International Law Applicable to Cyber Warfare* (CUP, 2013), p. 55; Schmitt M, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (CUP, 2017), p. 342.

635 'Droit international appliqué aux opérations dans le cyberespace' (*France, Ministére des Armées*) <https://www.defense.gouv.fr/sites/default/files/ministere-armees/Droit%20international%20appliqu%C3%A9%20aux%20op%C3%A9rations%20dans%20le%20cyberespace.pdf>, p. 3.

636 Netherlands: International Law in Cyberspace ((n 622), p. 4.

637 UNODA, 'Norway, Official compendium of voluntary national contributions' A/76/136 (2021), p. 69–70.

638 'Communication to the United Nations Human Rights Committee In the Case of SDG against Italy (Anonymized Version) Submitted for Consideration under the Optional Protocol to the International Covenant on Civil and Political Rights to The United Nations Human Rights Committee' (*GLAN*, 2019), p. 8.

639 ICJ, *Case Concerning Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America),* Judgment [1986] ICJ Rep 1986, paras 176, 194, ICJ, *Case Concerning Oil Platforms (Islamic Republic of Iran v. United States),* Judgment [1996] ICJ Rep 2003, paras 43, 73,74 and 76; ICJ, *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion [1996] ICJ Rep 1996, para 41, Judgment of the Nuremberg International Military Tribunal 1946 (1947) 41 *AJIL* 172, 435 – citing the Caroline test – see further e.g., Moore, Digest of International law, II, 24-30, 409-14; VI, 261-62; VII, 919-20.

criterion of necessity obligates the use of cyber force to be needed in order to defend the target State in a situation where the non-forceful measure would not suffice. The Tallinn Manual in this context asserts the necessity of primary usage of passive defense instruments (such as firewalls) and/or of non-forceful active cyber measures when the operations meeting the threshold of use of force are not inevitable. In case of a necessary use of force, the cyber means must adhere to the proportionate degree conditional on the situation in question – in terms of scope, scale, intensity, duration etc. On the contrary, there is simply no rule compelling the cyber self-defense to react to cyber-attacks only and *vice versa*.[640]

Another crucial aspect in the determination of legal exercise of self-defense is the issue of its imminence and immediacy. The States in their doctrines, as well as the scholarship, take different stances towards the concepts of preemptive (anticipatory) and preventive self-defense. The cyber context certainly does not detract from the controversy over this rather evergreen topic.

The collective form of the inherent right of self-defense naturally keeps its place in the cyber era,[641] as the capacities of States in the domain vary on a large scale. Needless to say, all the standard requirements applicable to the individual form, as well as additional established conditions for the collective self-defense, such as of a prior request of help, by the victim State, apply in a regular manner.

3. The question of attribution

Article 2(4) of the UN Charter only applies to uses of force that are conducted by States or are otherwise attributable to States. Attribution denotes "*the operation of attaching a given action or omission to a State*" under international law.[642] Under Article 2 of the Draft Articles on State Responsibility, crucially, attribution is one of the elements to finding an internationally wrongful act. Hence, all international claims are based on attribution. It is inferred if the actor is an organ of that State under Art 4 if the actor is exercising government authority under Art 5, or if the actor is acting on the instructions, or under the direction or control, of that State under Art 8. As a cornerstone of all international law, attribution must be applied, albeit with some difficulty, also to cyber-attacks and cyber espionage.[643]

While State-organs in the broadest sense are thus by definition attributable to the State in question, activities of non-State actors are generally non-attributable, if not

[640] Schmitt M, *Tallinn Manual on the International Law Applicable to Cyber Warfare* (CUP, 2013), pp. 61–62; Schmitt M, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (CUP, 2017), pp. 348–349.

[641] For more in a collective security organization perspective see, NATO 2020: Assured Security, Dynamic Engagement. Analysis and Recommendations of the Group of Experts on a New Strategic Concept for NATO' (17 May 2010), pp. 20 and 45 <www.nato.int/strategic-concept/expertsreport.pdf>.

[642] ILC, 'Draft Articles on Responsibility of States for Internationally Wrongful Acts' November 2001) UN doc A/56/10, Art. 3, para 12.

[643] Finlay L and Payne C, 'The Attribution Problem and Cyber Armed Attacks' (2019) 113 *AJIL Unbound* 202, p. 203.

under special circumstances. Accordingly, a plurality of tests has been developed over the years to tackle the attributability of often covert conduct of cyber operations.

In the principled *Nicaragua* case, ICJ concluded that a link of "effective control" between the State and non-State actors is necessary for attribution to be attained.[644] The degree of such control and the timeframe under which this control must be maintained has, however, been traditionally subject to much debate.

Organized groups have received a less restrictive treatment by the ICTY where both the qualitative and quantitative threshold has been lowered in order to facilitate the "overall control" test, which requires the State in question (i) to provide the non-State entity with financial and training assistance, military equipment and/or operational support, and (ii) to participate in the organization, co-ordination or planning of operations of the entity in question.[645] States are thus not required to directly participate in all individual attacks of an organized group in order to bear blame as long as their overall level of involvement is of a high enough intensity. This marks a clear dismissal of the *Nicaragua* case, where ICJ implied that attribution can only be granted as long as the State is able to control the beginning of the relevant operations, the way they are carried out, and their end.[646] Granted, the ICJ and ICTY differed in jurisdiction and the desired outcome of the proceedings, so the disagreement is less poignant than it seems at first.

Other traditional methods of attribution have generally been focused on State attribution of armed and terrorist groups engaged in kinetic warfare, with their State patron being either clandestine or entirely non-existent. In some instances, the power of these groups reached such an apex, that the opposite scenario became plausible, that is the effective control of such groups over the State they conduct their activities from. Suffice to say, these methods are ill-suited for cyber operations and will not be further elaborated on here.

Worthy of note is also the problem of attribution with regard to companies and enterprises which are partially or entirely State-controlled. In line with the principle of separateness between corporate entities on a national level, the fact that the State initially establishes a corporate entity, whether by a special law or otherwise, is not a sufficient basis for the attribution to the State of the subsequent conduct of that entity. In other words, whether the State is a partial or majority shareholder or the enterprise is entirely State-owned is not conclusive for attribution. Only when the State would exercise public power through the institution, or it would use its ownership share interest to maneuver the enterprise into specific action could attribution be inferred.

The Tallinn Manual takes on a different, *lex specialis*, approach to ease the way to *de facto* attribution. In line with the principle established in the *Corfu Channel* case - a State may not "*allow knowingly its territory to be used for acts contrary to the rights of*

---

644 ICJ, *Case Concerning Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America)*, Judgment [1986] ICJ Rep 392, para 115.

645 ICTY, *Prosecutor v. D. Tadić, Sentencing appeals in the case Dusko Tadic, CC/P.I.S./465-E (26 January 2000),* paras 120–121.

646 ICJ, *Case Concerning Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America)*, Judgment [1986] ICJ Rep 392, para 242.

other States"[647] - Rule 5 of the Manual provides that a State "*shall not knowingly allow the cyber infrastructure located in its territory or under its exclusive governmental control to be used for acts that adversely and unlawfully affect other States*".[648] Expert opinions differ on the rule's scope of application, whether it applies to cyber-attacks already underway or to those that are merely prospective. It is also uncertain whether State liability extends only to the territory of origin or also to "transitional" States.

The ephemeral nature of cyber-attacks has often been the main obstacle in inference of international liability with regards to the "attribution problem". It is a multi-faceted problem, encountering possible obstruction at every layer. First, an actor may mask their IP address using obfuscation techniques. Even if the location of the computer used to carry out the cyber operation were known, it does not definitively give away who was operating the computer. And even if the actor were identified, there would still be the obstacle of linking the actor to a State.[649]

Notably, the two most prominent cyber-attacks of the early and mid-2000s, namely the Stuxnet nuclear power attack and the Estonian cyber-attacks of 2007 were lacking an official apportionment of the blame, despite both resulting in serious destructive effect for the respective governments. Neither the Iranian nor Estonian governments issued an official statement regarding the incidents as neither had sufficient evidence linking the attacks to the foreign authority in question.[650]

Due to the unsatisfactory nature of rigid legal tests, more context-dependent approaches have allowed leeway in gathering and evaluation of evidence. It is generally acknowledged that any allegation that an internationally wrongful act has been committed must be sufficiently substantiated. Evidentiary standards for such substantiation have, however, not been harmonized and methods of proof are subject to individual State legal frameworks.

What's more, many States have officially subscribed to the notion that attribution of internationally wrongful acts engage various political considerations beyond the constraints of legal attribution standards and as such, the States do not bear an obligation to publicly provide the basis on which the attribution is made.

4. Controversy surrounding the Tallinn manual

At first glance, it would seem that the underregulated nature of cyberspace invites international legal regulation and the creation of a non-national space, in the vein

---

[647] ICJ, *Corfu Channel (United Kingdom of Great Britain and Northern Ireland v Albania)*, Judgment [1949] ICJ Rep 4, p. 22.

[648] Schmitt M, *Tallinn Manual on the International Law Applicable to Cyber Warfare* (CUP, 2013), p. 33, similarly the Rule 6 in Schmitt M, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (CUP, 2017), p. 30.

[649] Efrony D and Shany Y, 'A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice' (2018) 112 *American Journal of International Law* 583, p. 589.

[650] Macak K, 'Decoding Article 8 of the International Law Commission's Articles on State Responsibility: Attribution of Cyber Operations by Non-State Actors' (2016) 21(3) *Journal of Conflict and Security Law* 405, p. 409.

of Antarctica or the high seas.[651] However, States have traditionally been cautious in particular towards cyberspace regulation. The reasons for this reluctance are twofold:

Firstly, natural asymmetries in cyber warfare led to what some have called the *Glass house dilemma.* Powerful States are on one hand incentivized to opt for a more permissive system in which their technological edge allows for less restrictive manifestation of power. On the other hand, however, their overreliance on technology exposes them to new cyber threats from State and non-State actors with a fraction of their power. This leads to a legislative schizophrenia, where mutually exclusive interests collide and paralyzes those States that would ideally be at the forefront of any normative efforts.[652]

Secondly, the post-Tallinn practice showcased that States general stance towards the Tallinn manual is that of optionality. There are doubts whether the Manual is reflective of existing international law in the context of cyberspace, or merely the articulation of the views of an international group of experts on how international law *should* be applied.[653] Especially when such views are predominantly expressed by Western experts and only with limited State involvement.[654] Some Chinese observers have not hesitated to describe the Manual as a tool in hands of the US for manipulating the international legal process.[655] Conversely, there have been public statements from Western statesmen registered characterizing the Manual as aiding fostering State's positions and actions, or even as "the first step in codifying the cyberlaw".[656]

The Tallinn manual in effect touches on a much broader issue of the legitimacy of the role of experts in international law making. As it has been pointed out by the ICJ itself in the previously mentioned *Nuclear Weapons Advisory Opinion*, only the States have the power to create law.[657] In this regard, some authors argue that States naturally in their own interest refuse to delegate this function to others and overtly acknowledge an external normative source. On the other hand, this does not rule out any implicit inspirations in formulation of their future positions.[658] Yet the Tallinn Manual might instead simply represent the category determined by the art. 38, (1), (d) as the teachings of the most highly qualified publicists of the various nations.[659] After all, its role as

---

[651] Macak K, 'On the Shelf, but Close at Hand: The Contribution of Non-State Initiatives to International Cyber Law' (2019) 113 *AJIL Unbound* 81, p. 82.

[652] Ibid., pp. 82–83.

[653] Efrony D and Shany Y, 'A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice' (2018) 112 *American Journal of International Law* 583, p. 589.

[654] Luor T, Wang JF and Lu HP, 'Trends in and Contributions to Tallinn Manual Research: An Assessment of the Literature from 1998 to November 2022' (2023) 27 *Informatica Economica* 45, p. 46.

[655] See ex.: Ku J, 'Tentative Observations on China's Views on International Law and Cyber Warfare' (*Lawfare*, 26 August 2017).

[656] Kersti Kaljulaid, President of the Republic of Estonia (Keynote Speech at CyCon 2017, Tallinn, 31 May 2017); Stef Blok, Minister of Foreign Affairs of the Netherlands (Keynote Speech by the on First Anniversary of Tallinn Manual 2.0, 20 June 2018); Zoran Milanović, Prime Minister of Croatia, "Tallinn Manual is an Icebreaker" (NATO Cooperative Cyber Defence Centre of Excellence visit, Tallinn, 27 January 2015).

[657] ICJ, *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion [1996] ICJ Rep 1996, para 6.

[658] Tsagourias N, 'The Slow Process of Normativizing Cyberspace' (2019) 113 *AJIL Unbound* 71, p. 74.

[659] United Nations, Statute of the International Court of Justice, 18 April 1946, Art. 38, para 1, s. d.

subsidiary means for the determination of rules of law is to rather identify and prove the detailed content of the applicable rules of law - not being the source of law itself.[660]

Furthermore, due to the extensive diffusion and accessibility of the Manual, the upcoming generations of practitioners and advisors in the digital space are thus gradually learning about international law by reading the rules of the Tallinn Manual and their commentaries.[661]

Another more structural problem is that applicability of the framework of international law regarding the use of force to cyberspace has its limits. While there is an overwhelming consensus that international law is applicable to cyberspace, this seemingly does not translate well to all its logical conclusions. An example of this could be the ongoing academic debate surrounding self-defense embedded in Article 51 of the UN Charter. While the right to anticipatory defense can be argued for in a conventional kinetic use of force, it is much less conceivable to do so in a case of a cyberattack, despite the obvious double standard one is forced to adopt. Similarly, the suitability of the *jus ad bellum* and *jus in bello* duality to cyberoperations can be easily challenged.[662] Some have even gone as far as to question international law as a suitable normative framework for cyberspace, which seem to challenge conventional legal ways of defining *space*.[663] As a result, the formalistic legal approach of the manual may not be an appropriate means of combatting cyberspace and new, *sui generis* forms of cyber-governance should be developed instead.

Conclusion

Due to this plurality of obstacles in cyberspace, normative attempts have proven to be exceptionally cumbersome. States have so far demonstrated a skeptical view towards the Tallin Manual's utility in governing the law of cyberspace and have deployed a policy of strategic silence, highlighting the political nature of normativity in cyberspace.

Despite the multitude of criticism, the utility of the Tallinn Manual does not necessarily lie in accepting it as a codified set of laws. The importance of an existing material source of cyberlaw cannot be understated as it necessitates legal discourse and a venue for further normative opportunities. The Tallinn manual mirrors the frustration of legal practitioners with the innate unwillingness of traditional law-makers to legislate highly political issues.

Whether the Manual leads to a comprehensive *Cyber treaty* or not, it's worth lies in its ability to direct legal discourse in its field. The one-of-a-kind legal treatment of cyberspace fills a legal void which, in turn, necessitates its recognition in legal practice.

---

660 Yee S, 'Article 38 of the ICJ Statute and Applicable Law: Selected Issues in Recent Cases' (2016) 7 *J Int'l Disp Settlement* 472, p. 491.

661 Bannelier K, '"Rien Que La Lex Lata"? Étude Critique Du Manuel de Tallinn 2.0 Sur Le Droit International Applicable Aux Cyber-Opérations' (2017) 63 *Annuaire français de droit international* 121, p. 125.

662 Efrony D and Shany Y, 'A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice' (2018) 112 *American Journal of International Law* 583, p. 653.

663 Tanodomdej P, 'The Tallinn Manuals and the Making of the International Law on Cyber Operations' (2019) 13 *Masaryk U JL & Tech* 67, pp. 69-70.

This puts the Manual in a unique position in which even if States decide not to express acceptance, they are forced to express dismissal. Thus, the utility of the Manual, at least for the time being, lies in its unavoidability.

In the words of a former UK Attorney General Jeremy Wright: "*If we stay silent, if we accept that the challenges posed by cyber technology are too great for the existing framework of international law to bear, that cyberspace will always be a grey area, a place of blurred boundaries, then we should expect cyberspace to continue to become a more dangerous place*."[664]

[664] 'Cyber and International Law in the 21st Century' (*Gov.uk*, 23 May 2018).

5.3 Crossing Cyber Borders: Navigating a Path to International Cyber Defence

By ***Szymon Skalski*** (Jagiellonian University Krakow)

Introduction

Cyber-attacks present an expanding danger to the socio-economic stability of European societies as well as legal systems.[665] This issue cannot be attributed exclusively to an undefined fluctuation in human behavior in recent times. Even during the information revolution[666], humankind remains susceptible to disinformation and assaults by malicious entities. The phenomenon of networking has undoubtedly transformed the interpersonal space, facilitated by the widespread connection to the Internet through not just computers but also smartphones or IoT *(Internet of things)* devices. However, the industry is also vulnerable to a range of new threats, with numerous potential attack points including IoT and OT (*operational technology*) solutions, as well as the so-called IIOT (*industrial internet of things*).

The selected definition of cyber attack quoted below is notable for its global implication, the defining feature for the purposes of this article. Although the meaning of the word "global" is not in question, it has a distinct meaning in cyberspace. From a legal perspective, it is crucial to recognize that anyone, from anywhere in the world, can carry out a cyber attack. This serves as an important basis for subsequent discussions. In addition, the extent of the damage caused is a critical issue. In addition, the scale of the damage caused is a critical issue. In particular, the ENISA report highlights an almost 80% increase in the volume of data exposed between 2020 and 2021.[667] It is estimated that the stolen data amounts to more than 260 terabytes, containing more than 1.8 billion files, documents, or emails.[668]

The significant scale of cyber attacks and their extensive economic consequences compel states to pursue global agreement to tackle this issue. This article seeks to compare the 2001 Budapest Convention (BC),[669] widely regarded as the most crucial piece of international law concerning this domain, with the present UN-level draft Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes (Draft Convention, DC). [670]

---

665 ENISA, 'Threat Landscape 2022' (*European Union Agency for Cybersecurity*, 2022) <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022> accessed 7 October 2023.

666 Deitel H, Deitel B, *An Introduction to Information Processing* (Elsevier, 1986), p. 67.

667 Ibid., p. 67.

668 Ibid.

669 Council of Europe, 'Convention on Cybercrime' (Budapest, 23 September 2001) <https://rm.coe.int/1680081561> accessed 7 October 2023.

670 Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, 'Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes' (United Nations, 21 August – 1 September 2023) <https://www.undocs.org/A/AC.291/22>, accessed 7 October 2023.

Throughout history, public international law has primarily focused on conflict law, particularly armed conflict. Various publications have covered this topic.[671] Information warfare, hybrid warfare, and the activities of independent criminal groups present new challenges that have never been encountered before in international law. The Tallinn Manual 2.0,[672] published in February 2017, was a response to these issues. However, although this document holds great value in contributing to the understanding and practice of international law and will be extensively cited in subsequent research, it does not amount to an act of international law in the same manner as the international agreements mentioned previously. Rather, a specific piece of legislation must be sought for as an ultimate resolution instead of relying on guidelines. To achieve objectivity, this research study aims to conduct a comparative analysis of the existing proposed solutions. The paper intends to evaluate the progress made and determine whether the proposed mechanism is enough to achieve the objectives pursued by international law.

The adopted methodology involves discussing the formal and definitional issues related to the problem at hand. First, the cyber-attack itself will be defined and then placed in an international context. Next, the text will use categories as a basis for organizing the text, which are necessarily the basis for analyzing the issue of cyber-attacks in the context of international conflicts and will continue to be so in the future. These categories will be discussed comparatively on the basis of the current state of the law and the proposed changes to this regime at the UN level. However, the focus of the analysis will be on whether the envisaged international cooperation provisions have the potential to realistically address the global nature of the challenges posed by transnational cyber-attacks. Finally, conclusions will be drawn as to the shape and changes that the proposed UN Convention could bring to Europe and the world.

The main thesis of this text is that the current paradigm based on combating cybercrime through enumeration of crimes that together create a concept of cybercrime is ineffective and bares the critical mistake of transposing real-world solutions to cyberspace.

1. Background on Transnational Cyber-Attacks

Central to this research is the concept of a transnational cyber attack, which remains legally undefined. However, it is unequivocal that this refers to a cyber attack causing identifiable effects on multiple states. The inclusion of the identifiability clause is fundamental since cyber attacks, particularly those associated with terrorism, can result in significant international implications that are problematic to investigate. Identifying the definition of a cyber attack might seem straightforward, followed by the incorporation of an international perspective, and ultimately leading to the resolution of the definitional issue. However, this matter is unfortunately not as straightforward.[673]

---

[671] See in particular: Downey Jr WG, 'The Law of War and Military Necessity' (1953) 47 *AJIL* 2; Bassiouni MC, *International Terrorism and Political Crimes* (Springfield, 1975); Detter I, *The Law of War* (CUP, 2000).

[672] Schmitt M, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (CUP, 2017).

[673] It must be mentioned, that apart from regulations cited in this text there haven't really been any documents international level that address this matter precisely and satisfyingly. Most importantly it is hard to seek solution in any of the OECD documentation addressing the cybersecurity issues, namely: OECD, OECD,

However, starting with the simpler issues, the definition of a cyber attack should be briefly discussed. The first source of such definitions is through acts of international law. The BC does not directly indicate a definition of cyber attack. It does, however, refer to four categories of violations that it addresses. First, it refers in Titles 1 and 2 to violations consisting of computer-related offences. In particular, the obligation of signatory states to regulate was pointed out in Title 1: illegal access (Article 2 BC), illegal interception (Article 3 BC), data interference (Article 4 BC), system interference (Article 5 BC) and misuse of device (Article 6 BC). Subsequently, Title 2 defines computer related forgery (Article 7 BC) and computer related fraud (Article 8 BC). In conclusion, the provisions indicated illustrate quite well the catalogue of events that can be identified as a cyber attack. Surprisingly, the Draft Convention does not actually expand this catalogue in any meaningful way. The same categories are distinguished: unlawful access (Article 6 DC), unlawful interception (Article 7 DC), interference with computer data, digital information (Article 8 DC), interference with computer system, information and communication technology device (Article 9), misuse of devices (Article 10), computer forgery (Article 11), computer theft or fraud (Article 12). As can be observed, the process of extracting definitions with both conventions more than 20 years apart does not change. However, the two documents cannot be the same, as will be shown by a comparative analysis of further provisions of both conventions. The definitions shown above, derived from acts of international law, cannot be considered sufficient. Reference must therefore be made to international soft law. The best source in this regard would be the already mentioned Tallinn Manual. In accordance with Rule 92: *A cyber attack is a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects.* First, it should be noted that in international relations, especially in the context of conflicts between states in the digital arena, the inclusion of both offensive and defensive measures should be seen as an important added value. This is a very good example of how law should respond to the challenges posed by technology. On the one hand, there is a real distinction between offensive and defensive actions, which can be difficult to distinguish from the perspective of a participant in international relations. Moreover, it should be noted that this will not be the most important thing when analysing the responsibility of a particular entity or state for a cyber attack. On the positive side, the definition also includes a detailed explanation. This is because it is easy to find out important information about the scope of the definition. For the purposes of this research, it should be noted that this definition does not only cover the "release of kinetic force",[674] nor should damage to persons or property be used as an argument for not including the loss or destruction of computer

'Guidelines for the Security of Information Systems' (1992) <https://www.oecd.org/digital/ieconomy/oecdguidelinesforthesecurityofinformationsystems1992.htm> accessed 20 October 2023; OECD, 'Guidelines for the Security of Information Systems and Networks' (2002) <https://www.oecd.org/sti/ieconomy/oecdguidelinesforthesecurityofinformationsystemsandnetworkstowardsacultureofsecurity.htm> accessed 20 October 2023; OECD, 'Policy Framework on Digital Security' (2022) <https://www.oecd.org/digital/digital-security/> accessed 20 October 2023.

[674] Schmitt M, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (CUP, 2017), pp. 415-416.

data within the scope of this definition,[675] as stated in the Tallinn Manual. The above definitions are not ideal, but their flaws are quite different. The main criticism of the definitions that can be attempted by a process of reconstruction from the content of BC and DC is that a complex process of reconstruction is even required. Both acts define a number of terms: computer system, computer data, service provider, traffic data are for example defined in the BC. The DC adds to those definitions of content data, subscriber information, personal data, serious crime, child, property, proceeds of crime, freezing, confiscation, and predicate offence. What is missing from the catalogue, however, is a definition, a characterization of a cyber attack. Several key problems with such a solution can therefore be identified. Firstly, it forces the implementation of the DC principles into the orders of the signatory states on a very large scale. This causes a problem that can also be seen in the European Union when comparing the effectiveness of regulations and directives. If each state has to implement these solutions, far-reaching discrepancies will appear or, on the other hand, if an attempt is made to interfere extensively in the intellectual layer of criminal law in a given country, the solutions of the DC may prove impossible to implement in practice. Another example of the problems with such a definition are the far-reaching difficulties in modifying the adopted system. The need for constant fine-tuning of legal acts concerning cyber security can be seen, for example, in EU law, where the NIS Directive[676] has barely been implemented into the legal orders of the Member States and already had to be thoroughly reworked on the basis of the NIS2 Directive.[677] Relying on extremely general clauses makes them difficult to adapt. Of course, it can be argued that the original purpose of general clauses is precisely their generality, which allows them to be adapted to an ever-changing world. However, such an argument does not stand up to criticism in the field of cybersecurity. A good example is the phenomenon of ransomware: despite the plethora of regulations and the application of general sanctions for information security breaches throughout the Union, ransomware remains a problem and is unlikely to be solved without a tailor-made solution. This only underlines the phenomenon of ransomware being seen as illegal, using the analogy of kidnapping for ransom. This is a good example of how general criminal law norms diverge from the realities of cyberspace. One should therefore at least consider the approach proposed by some legal scholars, who advocate regulating these issues by influencing the architecture of the network, rather than solely through the letter of the law. The Convention has thus already missed an opportunity, which is not surprising given the timing of its creation, to regulate this issue in a functional manner. Nor can it be completely dismissed on the grounds that this approach was promoted by regulators in the years that followed. Unfortunately, it was also reflected in the draft proposed at the UN.

---

675 Ibid.

676 Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union [2016] OJ L194/1.

677 Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union [2022] OJ L333/80.

2. Illegal access

Illegal access was defined in BC as: *the access to the whole or any part of a computer system without right* (Article 2 BC). This might me supplemented with the provisions that make a finding that an offence has been committed subject the fact whether it was *committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system* (Article 2 BC). This article was widely criticized already at the level of the draft convention submitted in 2000.[678] The generality of the statement 'without right' was pointed out in particular.[679] From today's perspective, this criticism can only be expanded while acknowledging its accuracy. With the development of the internet and cyber security, a number of technological solutions are emerging, exploited by White Hat, Black Hat and Grey Hat hackers alike. Moreover, within organizations, both the Blue Team and the Red Team are using a number of technological solutions that could de facto be considered to meet the standard indicated in this discussed section of the convention. It should also be pointed out that there is a specific grey area of hacktivism, which often balances on the edge of the law. However, the biggest criticism that can be levelled at the solution is the failure to take into account the specific nature of cyber-attacks themselves. In a non-exhaustive list, the types of attacks whose main objective is to gain access to data can be identified: phishing, Brute Force Attacks, MitM (Man in the Middle) Attacks, Zero days, XSS (Cross-Site Scripting) or perhaps most importantly the umbrella term that is malware. It may be argued that, after all, it is the generally worded clause that allows all relevant cases to be 'caught'. To refute such an argument, it suffices to compare two extremely different types of cyber attacks. On the one hand we can put malware, on the other two interesting types of cyber attack: Side-channel attacks and Clickjacking. The term malware, which is an abbreviation of the phrase malicious software, is attributed to computational scientist Yisrael Radai.[680] However, the term has been expanded in later years, right up to the present day. From today's perspective, programs that were limited to generating the message 'I'm the creeper, catch me if you can'[681] might seem simple and crude yet we have reached an era of cyber-attacks supported by the infrastructure of entire countries and managed by both military and international hacking groups.[682] The term therefore encompasses a range of events, however, it can be simplified, for the purposes of this research to: "any code added, changed or removed from a software system in order to intentionally cause harm or subvert the intended function of the system".[683]

[678] See opinions of Centre for Democracy and Technology cited in: Baron R, 'A Critique of the International Cybercrime Treaty' (2002) 10 *CommLaw Conspectus* 263, p. 278.

[679] Ibid.

[680] Radai Y, 'The Israeli PC Virus' (1989) *Computers & Security*, pp. 111–113.

[681] See blogpost: 'Core War: Creeper & Reaper' (Core War, 2020) https://corewar.co.uk/creeper.htm, accessed 20 October 2023.

[682] On the history of malicious software see: Saengphaibul V, 'A Brief History of The Evolution of Malware' (*Fortiguard Labs Threat Research*, 2022) <https://www.fortinet.com/blog/threat-research/evolution-of-malware> accessed 20 October 2023.

[683] Idika N and Mathur A, 'A survey of malware detection techniques' (*Purdue University*, 2007) <https://www.researchgate.net/publication/229008321_A_survey_of_malware_detection_techniques>, p. 48.

The first type of attack that can be problematic from the perspective of the definition of illegal access in BC are so-called side channel attacks. Side-channel attacks exploit information from the physical attributes of a cryptographic system rather than its algorithmic flaws. Attackers can decipher the secret key by analyzing variables like timing, power consumption, and electromagnetic emissions.[684] Depending on how this is interpreted in the particular country implementing the Convention, we may understand the wording about gaining access to a computer system differently. As a result, this type of attack will be considered a crime in one country, but not in another. This is due to the fact that, according to the current position of cryptographic sciences, it is difficult to actually speak of a specific gaining of access. The other mechanisms provided for in the BC will also not apply here. A slightly different problem of the aforementioned definition is posed by so-called clickjacking. This involves getting users to click on a target other than the one they perceive by overlaying a malicious interface on a legitimate page. For example, an attacker may superimpose a transparent frame over a legitimate button, causing users to perform an unwanted action.[685] Quite why this attack is also difficult to include in this definition is obvious. This is because it is difficult to identify a moment in time when access to a computer system is gained. Everything de facto happens via the network architecture.

Returning to the present day, however, one wonders whether the currently proposed Convention (DC) addresses the problems identified on BC grounds. The short answer is no, admittedly a more elaborate conceptual grid has been intro, which has been introduced on DC grounds, but without much change. The biggest change in the DC text with respect to the version proposed in the BC is the inclusion of editorial units which makes it much easier to read.

3. Illegal interception, data and system interference

The other three types of infringement described successively in Articles 3 (illegal interception), 4 (data interference) and 5 (system interference) are *de facto* extensions of the presumptions established under Article 2 BC. Unfortunately, analogous allegations can be made against them. They will be presented briefly because of the purpose of this research and the repetition of the allegations made against these definitions - as they are very similar to the allegations made against the Article 2 definitions.

The definition of illegal interception proves problematic when we often consider situations in which content is accidentally made public. Although they may be hidden to the ordinary internet user, de facto they are publicly available and can be accessed without breaking any security or using social engineering techniques. Examples of such popular solutions are various types of search engines, which can be used to find vulnerabilities in, for example, the Internet of Things.[686] Examples include images

[684] See more in: Prabu M, Shanmugalakshmi R, 'An Overview of Side Channel Attacks and Its Countermeasures using Elliptic Curve Cryptography' (2010) 2 *IJCSE* 1492.

[685] See more at: Chiarelli A, 'Clickjacking Attacks and How to Prevent Them' (*Auth0 Blog*, 2020) <https://auth0.com/blog/preventing-clickjacking-attacks/> accessed 20 October 2023.

[686] Probably the best example is Shodan, https://www.shodan.io/, access: 22.10.2023, which can be used in variety of ways by both good and malicious actors. For more on Shodan see: Chen YY et al, 'Exploring

from e.g., CCTV cameras. It can be assumed that camera owners would not want their images to be available everywhere, but security flaws result in images being made available to the public. Is or should it be against the law to use such information? This will of course depend on the country in question, but one can probably agree that if it is used for research purposes or to enhance the security of an organisation such use should not be considered illegal. However, the line is a fine one and such a framing of Article 3 should be considered problematic. Very similar arguments can be made on the grounds of man-in-the-middle attacks. This type of attack occurs when an attacker intercepts a conversation between two parties, either to eavesdrop or pose as one of them. Mobile devices are particularly vulnerable, as attackers can introduce false information like bogus certificates during secure connection attempts. This can result in users being redirected to unsecured sites or being deceived by fake encryption keys in a key exchange process.[687] It's obvious that the act could constitute illegal interception, but it could be argued that if the transmission was made publicly available by accident, or if the attacker was inadvertently placed in the middle, then it could not be considered "intentional".

Data and system interference can be addressed as one. Indeed, the problems are similar enough. Firstly, the lack of definition of data should be pointed out. This may have been due to the low level of awareness at the time regarding, for example, the importance of metadata.[688] Secondly, and most importantly, there is no indication of the methods by which the infringements in question may be carried out. This gives a great deal of scope for law enforcement agencies, which must demonstrate a very high level of technical expertise to adequately scale down unwanted behavior. Finally, one can add the problematic nature of the phrases 'inputting' and 'transmitting', which in themselves are not usually contrary to the law. This may lead to further complicating the application of this provision.

For the second time, it must be stated that, unfortunately, DC does not provide material for a comparative analysis of these provisions. This is because they have been practically rewritten without any significant modification to the content of the DC.

4. Misuse of device

Article 6 BC, which statutes a standard prohibiting the production and use of hacking devices and software, has been widely criticized since the BC = adoption.[689] Nothing to the criticism needs to be stated as of today, except perhaps the fact that the number of such tools, including within the open-source movement, has increased

Shodan From the Perspective of Industrial Control Systems' (2020) 8 *IEEE Access*; Genge B, Enăchescu C, 'ShoVAT: Shodan-based Vulnerability Assessment Tool for Internet-facing Services' (2016) 9 *Secur. Commun. Netw.* 2698.

687 Oriyano SP and Shimonsky R, 'Mobile Attacks' in Oriyano SP and Shimonsky R, *Client-Side Attacks and Defense* (Elsevier, 2013), p. 238.

688 This remark is due to the fact that despite the existence of metadata in the general consciousness, see above all the standard: IPTC7901 from the year 1979 <https://iptc.org/standards/iptc-7901/> accessed 22 October 2023. The importance of metadata has been brought up to public attention only few years back.

689 Baron R, 'A Critique of the International Cybercrime Treaty' (2002) 10 *CommLaw Conspectus* 263, pp. 271–273.

dramatically. As part of the criticism, it was pointed out that such a formulation could prevent the production not only of devices that could be used exclusively for hacking but also of devices that could only potentially be used for such purposes. *Ad absurdum*, it could be argued that, based on such a wording, one could probably argue for a ban on the use of computers, which would certainly solve the problem of cybercrime. Of course, this article is not rescued by the statement in paragraph 2 exempting from liability the creator, purchaser or seller who does not act with malicious intent. Such an exemption might as well not exist, as it is entirely discretionary and de facto does not solve any problem.

This provision has also been fully "recycled" in DC.

5. Possible expansion of scope

The above enumeration is not a complete recounting of the structure of the crimes enumerated in BC and DC. Both pieces of legislation include several other crimes, particularly those related to sexual offenses and child pornography. However, they do not represent, to any significant extent, an illustration of a cyberattack per se. In fact, they focus only on the effects, not the methods. And it is the methods that are the focus of this study.

It should be pointed out, however. that currently 11 crimes can be identified on DC soil. In the first proposals they appeared around 30. This is a significant reduction, which should be considered rather favorable. After all, excessive casuistry can contribute to far-reaching violations by law enforcement agencies of countries that do not guarantee a high level of protection of human and civil rights. It should be pointed out, however, that a certain dangerous casuistry has been encoded in the structure of the DC. It is mentioned firstly in paragraph 3 of the preamble and secondly in Article 17. According to Article 3 of the DC preamble, states are concerned about the impact that information technology has on the commission of other crimes, particularly those with a terrorist background. Article 17 mandates that States Parties adapt their laws to ensure that offenses recognized in international conventions also apply to crimes committed using computer systems or information and communications technology devices. Both provisions seem harmless, but express a certain tendency, to leave the catalogue of activities covered by the convention and the exchange of information provided for therein, which can be dangerous. This is because it allows States to expand the scope of the Convention virtually at will.

6. Effectiveness of proposed approach

To begin with, to evaluate the effectiveness of the adopted mechanism, it is important to provide a clear definition. The approach, which was proposed over 20 years ago in BC, relied on an enumerated list of cybercrime types. The approach discussed has been fully embraced on DC grounds. It is assumed in this text that this was a deliberate approach, and that the creators of the Convention intended to define the characteristics of a cyber attack in this manner. Therefore, it is necessary to assess how successful this approach will be, based on the argumentation. This section of the paper will present

the advantages and disadvantages of the approach and recommend a course of action. As an undoubted advantage of the proposed approach, it should be pointed out that the enumeration of cybercrimes undoubtedly facilitates the implementation of such provisions in domestic law. In fact, it is difficult to imagine a simpler approach. However, while one should agree with the statement that international law should strive for an appropriate level of generality so that diverse legal systems can comply with it, this rule cannot be applied blindly. As indicated in the above argumentation, a mechanism that is too simple will necessarily fail to cover the key nuances of the regulated facts.

Related to the above advantage is a more specific issue and that is the creation of a scheme, virtually ready for implementation by countries around the world. Nothing in these provisions is revolutionary (we are, of course, referring only to the provisions on the definition of crimes), but the way they are drafted creates a relatively coherent system that, with appropriate modifications, can be translated into national law. In this respect, a similar success of DC as BC can be expected, as can be seen from an analysis of the implementation reports[690], the assumptions of BC, at least formally, have been implemented into national law.

One of the primary challenges with this approach is its tendency to quickly become outdated in the face of rapidly evolving cyber threats. The digital landscape is constantly changing, with new forms of cyber-attacks emerging at a pace that often outstrips the ability of legislative processes to keep up. Consequently, laws based on the enumeration of specific types of cybercrime can become obsolete almost as soon as they are enacted. Obsolescence is not only a theoretical concern, but it also has practical implications for law enforcement and cybersecurity efforts. New threats that do not fit neatly into predefined categories risk falling into legal grey areas, making it difficult for authorities to prosecute these cases effectively.

Additionally, the enumerative approach may inadvertently stifle the law's ability to adapt to future technological advances. Laws that focus on specific methods and types of cyber-attacks prevalent at the time of enactment may lack the necessary flexibility to address future technologies and methods. This rigidity can hinder the development of legal frameworks that are responsive to the dynamic nature of technology and cybercrime. Cybercrime laws can become reactionary, constantly playing catch-up with cybercriminals instead of proactively anticipating and mitigating emerging threats.

While the enumerative definition of cybercrime provides clarity and specificity, it also presents challenges such as the risk of rapid obsolescence, the creation of legal gaps, and the stifling of legal adaptability to technological advances. To address these issues, it is necessary to re-evaluate the approach and consider more dynamic and flexible legal frameworks that can adapt to the constantly evolving cyber landscape. This adaptation is essential to ensure that legal responses remain effective and relevant in the face of the ever-changing nature of cyber threats.

[690] Council of Europe, 'Assessing the implementation of the Budapest Convention' <https://www.coe.int/en/web/cybercrime/assessments> accessed 16 December 2023.

Conclusion

The current paradigm for combating cybercrime, based on enumerating specific offenses to form a comprehensive concept of cybercrime, has demonstrated notable inefficiencies. This approach, while providing clarity and specificity, struggles in the face of the rapidly evolving nature of cyber threats, leading to legal frameworks that become outdated almost as soon as they are enacted. The challenge is exacerbated by the attempt to transpose solutions from the physical world into the complex and dynamic realm of cyberspace, a process fraught with difficulties due to the unique characteristics of cyber threats.

One critical flaw in this approach is its inherent rigidity. As cyber threats evolve and new forms emerge, laws based on specific types of cybercrime quickly fall into obsolescence. This not only creates legal gaps, making it challenging for authorities to effectively prosecute new forms of cybercrime, but also stifles the ability of the legal framework to adapt to future technological advances. The dynamic nature of technology and cybercrime necessitates legal responses that are equally dynamic and flexible, capable of adjusting swiftly to new developments.

The need for global cooperation and comprehensive strategies is underscored by the transnational nature of cyber-attacks. Effective combat against cybercrime requires international conventions and agreements that are inclusive and adaptable, acknowledging the diverse and evolving nature of cyber threats. This includes a better integration of technological understanding with legal strategies, ensuring that laws are not only robust but also reflect the realities of modern technology.

For instance, emerging threats like ransomware and various forms of malware highlight the need to address the gaps and ambiguities in current legal definitions of cybercrimes. Concepts like illegal access, interception, and data interference need to be redefined in the context of the contemporary digital environment. It is essential that legal frameworks emphasize preventive measures and adaptability, equipping them to stay ahead of cybercriminals through continuous updates in response to emerging threats and technological advancements.

A rethinking of cybersecurity legislation is thus imperative. Moving away from traditional, static legal approaches to more nuanced, flexible, and technology-informed strategies is essential. This shift involves recognizing the unique challenges of the digital landscape and crafting laws that are not only comprehensive but also capable of evolving with the rapid pace of technological change. This re-evaluation must focus on creating laws that are robust and detailed, yet flexible enough to address the ever-changing nature of cyber threats.

In conclusion, the text underscores the urgency of reevaluating and updating legal frameworks in response to the dynamic nature of cyber threats. A shift from traditional, static legal approaches to more adaptable, technology-informed strategies is essential for effective cybersecurity legislation. This involves a comprehensive understanding of the technological aspects of cyber threats and tailoring legal responses accordingly. By embracing a more dynamic and flexible legal framework, we can ensure that our responses to cybercrime are effective, relevant, and up-to-date in the face of the constantly evolving digital landscape.

CHAPTER VI

CYBER-SECURITY AND CYBER-DEFENSE

6.1 Violations of the International Law Standards on Cyber Security in Ukraine

By ***Agata Starkowska*** (University of Warsaw)

Introduction

For almost two years, today's international reality has been marked by one of the most notorious armed conflicts of the 21st century, the Russian-Ukrainian war. Having taken into account the data published in the global reports, we can provide that the total number of dead and wounded soldiers in Russia's war against Ukraine has approached 500,000 so far.[691] The scale of the problem is further emphasised by the number of civilians affected. All this does not enable us to adopt an indifferent attitude towards the war being waged today. The subject of this article was also prompted by the clear connection of Poland, the country of origin of the author of this publication, to the fate of the ongoing war. This observation is evidenced by the location of Poland near the border of the aggressor and defender, even in the immediate vicinity of the ongoing battles.

Nevertheless, the most important factor prompting the issue of the Russian-Ukrainian war is the very nature of the war itself. Indeed, this war is an example of hybrid war in the broadest sense. This type of conflict eludes conventional operations because it contains an element of modernity abounding above all in technological and economic progress. For the purposes of this paper, the analysis carried out will refer to the thread of cyber-related breaches being an important element of hybrid war.

The doctrine emphasises that Russia is one of the pioneers when it comes to carrying out cyber attacks and hybrid wars.[692] The origins of such operations by this country date back to the 1980s. The first known espionage cyber-attack carried out by Soviet services at the time, was the hacking of the computer system handling missile tests of Ronald Reagan's flagship strategic defence. The operation became known in history as Star Wars, and was dated 10 September 1986.[693] Forthermore, a post-2016 investigation found that it is likely that Russia also tried to influence the outcome in the US presidential election betweenHilary Clinton and Donald Trump. Attempts were made to influence US voters through social media and troll farms paid for by the Kremlin troll farms (including the St Petersburg-based Russian organisation Internet Research Agency).[694]

The Russian-Ukrainian conflict therefore represents the next stage in Russia's expansion concerning cyberspace. It should be underlined that in the 21st century, Russia has

[691] Górzyński O, 'Ile osób zginęło na Ukrainie?' (*Wszystkoconajwazniejsze*, 18 August 2023) <https://wszystkoconajwazniejsze.pl/pepites/ile-osob-zginelo-na-ukrainie-3/> accessed 16 December 2023.

[692] Gardocki S, Wrona J, 'Russia's use of cyberspace in hybrid conflicts in the light of Russian cyber security policy' (2020) 2(38) *Colloquium* 33.

[693] 'Imperium zła. Doktryna Regana wciąż aktualna?' (*Historia dorzeczy*, 9 March 2022) <https://historia.dorzeczy.pl/273418/imperium-zla-doktryna-reagana-wciaz-aktualna.html> accessed 16 December 2023.

[694] Gardocki S, Wrona J, 'Russia's use of cyberspace in hybrid conflicts in the light of Russian cyber security policy' (2020) 2(38) *Colloquium* 33.

already taken actions against Ukraine which are part of the hybrid war concept. This observation refers to the events at the beginning of the second decade of the century.[695]

The confrontation of contemporary regulations of international law with contemporary methods of action of states involved in armed conflicts will consequently seek to answer the question of how far today's legal framework reflects current reality. In result, therefore, the reflections carried out are intended to examine the state of contemporary international law.

Due to the currency of the issue addressed in the article, the primary source on which the analysis is based is journalism enriched by the perspective of legal acts and statements of doctrine.

Concept of the 'cybersecurity' and the 'hybrid war'

It would be undoubteldy difficult to create and use only one definition of 'cybersecurity'.[696] Each national system has its own one and there are also a lot of descriptions given by the doctrine of law. For example, the definition used in Polish regulations, that is very close to the author of this paper, sounds: that the 'cybersecurity' is 'the resistance of the information systems to actions that affect the confidentiality, integrity, availability and authenticity of the data processed or the related services offered by the systems'.[697]

When it comes to the doctrine we can notice that more frequently there are some definitions realted to the concept of 'the hybrid war' part of which is the violation of the aforementioned cyber security. For example, Frank Hoffman points out that hybrid war is 'any adversary that simultaneously employs a tailored mix of conventional weapons, irregular tactics, terrorism, and criminal behavior in the same time and battlespace to obtain their political objectives'.[698]

Focusing on the analysis of the concept of hybrid war on doctrinal grounds seems to support the thesis that the concept is a product of legal language and legal science. Rather, cyber war is a technical concept, for which a definition is more easily created on the basis of the legal system. This is because hybrid war is a conglomeration of contemporary methods of fighting a war opponent.

The indication of the above definitions is of an orderly nature and its primary function is to provide some perspective from which to view the regulations analysed below.

1. The international standards aimed at ensuring cyber security

At the beginning, it has to be underlined that international law does not explicitly regulate hybrid war. It is therefore impossible to list unified and universal mechanisms

[695] Hajduk J and Stępniewski T, 'Russia's Hybrid War with Ukraine: Determinants, Instruments, Accomplishments and Challenges' (2016) 2 *Studia Europejskie – Studies in European Affairs* 37.

[696] Worona J, *Cyberspace and International Law – Status Quo and Prospects* (Białystok, 2017).

[697] Art. 2 p. 4 of Polish Act of 5 July 2018 on the national cyber security system.

[698] Hoffman F, 'On Not-So-New Warfare: Political Warfare vs Hybrid Threats' (*War on the Rocks*, 28 July 2014) <http://warontherocks.com> accessed 21 October 2023.

for responding to the behaviour of states that may be a manifestation of cyber attacks.[699] It is intended to return to the topic of responses in the form of sanctions to violence in cyberspace later in the paper.

We need to agree with the Sylwester Gardocki and Joanna Wrona who said that: 'Assigning responsibility for a traditional armed attack is relatively easy, while in the case of the use of cyberspace it is very difficult and sometimes impossible. Virtual space offers aggressors the opportunity to cover their tracks and exploit the IT infrastructure of a of a third party. Countries blamed for an attack often distance themselves from the hacking group that carried out the operation, denying any association'.[700] That is the reason why cyber attacks are still one of the most difficult to catch and describe type of agression. Therefore they seem to be worth analysing from the scientific point of view.

However, we can still point to some regulations that are associated with the cyberatacks and the hybrid war. First of all, the attention should be drawn to the the provisions of the UN Charter. Indeed, these provisions are binding when it comes to Russia.

For instance, Agata Małecka mentioned that 'the UN Charter, that in Article 51 is act-based, does not include cyber-operations, because they do not generate negative effects by release of kinetic force. However, it should be considered that the intention of the drafters of Charter was to avoid certain effects, that is, to discourage states from initi-ating armed attacks, which consequences for the affected states were severe enough to respond militarily as well. This consequences-based approach means that all cyber--operations with effects analogous to those caused by kinetic actions consideredas an armed attack will also be treated as an armed attack'.[701]

Moreover, in her article there is a reference to the prohibition of the use of force in international relations, which is based on Article 2(4) of the UN Charter. This regulations should be also taken into consideration when it comes to the potential cyberconflict.

Sven Herpig from the German foundation named Stiftung Neue VerantwortungIf who specialises in cyber issues claimed that the effects of a cyber operation were equivalent to an armed forces operation, then the cyber operation would also result in a violation of Article 5 of the UN Charter.[702] In his opinion, the means used do not matter, only the effect counts.

It needs to be mentioned that one of the most important international acts relating to crimes committed in cyberspace is the Convention on Cybercrime of 23 November 2001. Despite this title, the doctrine points out a huge defect as to the content, which refers primarily to common crimes without addressing espionage or cyber military activities.[703]

---

[699] Gardocki S, Wrona J, 'Russia's use of cyberspace in hybrid conflicts in the light of Russian cyber security policy' (2020) 2(38) *Colloquium* 33.

[700] Ibid.

[701] Małecka A, 'Cyber operations under international law' (2022) 3(47) *Colloquium* 149.

[702] Taube F, 'Wojna w Ukrainie. Szczególna rola cyberataków' (*DW*, 1 March 2022) <https://www.dw.com/pl/wojna-w-ukrainie-szczeg%C3%B3lna-rola-cyberatak%C3%B3w/a-60957901> accessed 16 December 2023.

[703] Gardocki S, Wrona J, 'Russia's use of cyberspace in hybrid conflicts in the light of Russian cyber security policy' (2020) 2(38) *Colloquium* 33.

However, it has to be underlined that as regards the UN, it is noted that it is constantly working on the development of concrete standards and regulations strictly applicable to cyber security issues.

The most crucial cyber issues were discussed, for instance, on the sessions organised by the Groups of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security and Open-Ended Working Group on Developments in the Field of ICTs in the Context of International Security.[704] The genesis of the above-mentioned structures dates back to 2003, when the UN General Assembly asked the Secretary-General to analyse potential threats to information security and, as a result, a subsequent publication relating to possible preventive measures and cooperation opportunities that would help to minimise the risks associated with cyberspace.

The last one was conducted in an open-ended format, meaning that any UN member state could become involved in its work. At the same time, consultations took place with representatives of the business world, NGOs, and academics.

In addition to the role of regulations and the outcome of UN and NATO summit sessions, EU legislation may also be applicable in the context of cyber conflict. Obvously, we should point out the Directive[705] adopted on 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

Under this act, the EU Member States were obliged to carry out three key tasks. Firstly, each country was obliged to establish competent authorities (National Competent Authorities). The task of the Competent Authority is to monitor the implementation of the Directive's provisions at national level in all regulated sectors. Secondly, the Directive introduces mechanisms for inter-state cooperation at the technical level – i.e. to be ensured through the so-called CSIRT network and the creation of mechanisms for the exchange of information on cross-border incidents between CSIRTs designated for key service operators and digital service providers. The next level is the political and strategic level, which is to be implemented through the establishment of a so-called Cooperation Group, which is to deal with the development of common strategic concepts and the acceptance of, among other things, annual reports from the competent authorities.[706]

Although the EU regulations do not apply to and are not directly binding on Russia and Ukraine, which are outside EU structures, by binding the Member States they provide an important frame of reference for the perception of conflicts related to cyber-

[704] Balcewicz J, 'UN GGE - Prawo międzynarodowe w cyberprzestrzeni' (*NASK*, 15 January 2020) <https://cyberpolicy.nask.pl/un-gge-prawo-miedzynarodowe-w-cyberprzestrzeni/> accessed 16 December 2023.

[705] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union [2016] OJ L194/1.

[706] Wrzostek M, 'Dyrektywa NIS, czyli pierwsze europejskie prawo w zakresie cyberbezpieczeństwa' (*NASK*, 6 July 2016) <https://cyberpolicy.nask.pl/dyrektywa-nis-czyli-pierwsze-europejskie-prawo-w-zakresie-cyberbezpieczenstwa/> accessed 16 December 2023.

space. For it is not so much about rigid regulations as it is about the 'spirit' of the regulations, as the Court of Justice of the EU often emphasises in its judgments.

2. The violations of the abovemetntioned regulations during the Russian-Ukrainian conflict

Some examples of security violations in cyberspace have been seen since the very beginning of the war.[707] And even before the outbreak of the conflict (sic!), there were repeated attacks from Russia. It might therefore be argued that the hybrid war was primary to the actual armed conflict fought since February 2022. For instance, one of the most recognisable situation was registered on 15 February 2022. The websites of the Ukrainian Ministry of Defence, the armed forces and the two largest state-owned banks (PrywatBank and Oszczadbank) were attacked. The attack consisted of overloading the servers with artificially generated queries to lead to difficulties in accessing government websites, online banking and the bank's mobile app. Some payment systems were also visibly impaired. As The Polish Institute of International Affairs mentioned, the aim of this attack was not to obtain information, but to sow panic in society. The blocking of websites should have probably led to lowering Ukrainians' confidence in the state's defence capabilities. Moreover, the attack on banks was in turn intended to undermine confidence in the financial system.

As an interesting aside confirming the scale of the problem, it may be pointed out the firm Check Point Research, in its 2023 Cyber Security Report, stated that the number of cyber attacks on the Ukrainian government and military sector in the first three days of the war increased by 196% and the number of phishing messages in Eastern Slavic languages increased by as much as seven times.

The function that can be attributed to cyber attacks is therefore interesting. Taking as a given the primary role that this type of behaviour is intended to play, it is not possible to conclude *a priori* that it is about the acquisition and theft of information. Using the example of Russia's action described above, it is evident that often the basic premise of the groups responsible for carrying out a cyber attack is to influence the psyche of the authorities and society as a whole. Thus, the cyber attack is intended to create a space susceptible to further military and economic action. In this light, the fact that cyber attacks often occur before the outbreak of a proper interstate conflict seems to find justification.

Since the beginning of this year, nearly 4,000 cyber-attacks have been recorded.[708] Despite their scale, it should be emphasised that, Russian cyber attacks are being met with an increasingly advanced response from the Ukrainian services. For instance, there is a special organisation named The Security Service of Ukraine (reffered to as: '**SSU**') which fights against cyber attacks.

---

[707] 'Cyberatak na Ukrainie. Celem hakerów było czyszczenie danych' (*Wydarzenia*, 23 February 2022) <https://www.rp.pl/polityka/art35745821-cyberatak-na-ukrainie-celem-hakerow-bylo-czyszczenie-danych> accessed 16 December 2023.

[708] Palczewski S, 'Ataki na Ukraine. SBU podało dane za ten rok' (*CyberDefence 24*, 4 October 2023) <https://cyberdefence24.pl/armia-i-sluzby/ataki-na-ukraine-sbu-podalo-dane-za-ten-rok> accessed 16 December 2023.

The SSU organised a seminar for information security personnel in government bodies and strategic entities.[709] During this seminar, the participants developed algorithms for cooperative action to react and minimise the negative effects of relevant cyber attacks.

Another Ukrainian response to cyber attacks from Russia was to get help from the worldwide informal hacking movement 'Anonymous'.[710]

Moreover, the SSU connected the systems of more than 1,700 government structures and strategic facilities to a specialised MISP-UA platform for sharing information about detected incidents.

3. Some sanctions, in particular technological ones

It is impossible not to address the issue of sanctions in response to Russia's actions when discussing violations. The framework of this paper only allows for a selective focus on sanctions, so it seems justified to take an EU perspective, as we have adopted a European perspective on the Russian-Ukrainian conflict from the outset of the interview. In principle, EU sanctions can be divided into individual, economic and diplomatic. EU sanctions are designed mostly to weaken Russia's economic base: depriving the country of access to critical technologies and markets and significantly reducing its war-making capabilities.[711]

When it comes to the individual ones, we have to notice that EU individual sanctions currently apply to almost 1 800 individuals and entities, such as banks and financial institutions, military and defence companies, companies in the aerospace, shipbuilding and mechanical engineering sectors, armed forces and paramilitary groups, political parties.

Among the economic sanctions, which interestingly already took place at the beginning of the first decade of the 21st century during the first Ukraine-Russia crisis, were: restricting Russia's access to EU capital and financial markets banning transactions with the Russian Central Bank banning the delivery of euro banknotes to Russia. Others include, for example, a ban on oil and coal imports from Russia and a price ceiling related to the maritime transport of Russian oil, closure of EU skies to all Russian aircraft and entry ban for Russian road hauliers.

The most interesting and relevant to the topic of the study appear to be the technological and media sanctions, which include, for example, from 2022, the suspension of broadcasting activities and licences of a number of Kremlin-backed broadcasters sprea-

[709] 'Od początku roku SBU zneutralizowała prawie 4 tys. cyberataków na władze i infrastrukturę krytyczną Ukrainy' (*Security Service of Ukraine*, 3 October 2023) <https://ssu.gov.ua/novyny/z-pochatku-roku-sbu-neitralizuvala-maizhe-4-tys-kiberatak-na-orhany-vlady-ta-krytychnu-infrastrukturu-ukrainy> accessed 16 December 2023.

[710] Taube F, 'Wojna w Ukrainie. Szczególna rola cyberataków' (*DW*, 1 March 2022) <https://www.dw.com/pl/wojna-w-ukrainie-szczeg%C3%B3lna-rola-cyberatak%C3%B3w/a-60957901> accessed 16 December 2023.

[711] Council of the European Union, EU sanctions against Russia, Press release <https://www.consilium.europa.eu/en/policies/sanctions/restrictive-measures-against-russia-over-ukraine/> accessed 16 December 2023.

ding disinformation such as Sputnik and subsidiaries, including Sputnik Arabic, Russia Today and subsidiaries.

4. The Cybersec Forum in Katowice

Finally, it is high time to discuss the event that took place in Katowice on 21/22 June this year.[712] It was an annual public policy conference on the strategic aspects of cyber security related to the global technological revolution.[713] Although this topic is of marginal importance for the key deliberations, it shows how important the situation in Ukraine is in the context of the global economy and politics, including Poland. In particular, one has in mind here operations related to cybercrime.

It should be noted that among the measures discussed at the forum were projects proposed by the Ministry of National Defence. For example, there are some interesting solutions aimed at youth. At the Military University of Technology, the number of places on the cryptology and cyber-security course was increased fourfold. In addition, a programme called 'CYBER.MIL' with a class' has been launched even before Europe embarks on the path of armed conflict, as early as April 2020. Its main aim is to educate future cyber security experts. Schools interested in participating in the programme were able to apply to set up classes at their institution with a special profile that prepares them precisely for work in military and technology ministries. This mainly involved running classes with extended teaching profiles in mathematics and computer science or physics, as well as teaching and educational activities in the field of national defence.[714]

Leaving aside the military and economic aspects, which were also not absent from the Katowice summit, it is worth looking at the functionality of the idea of betting on the education sector in the context of the fight against cyber attacks, emphatically highlighted at the event. This trend is undoubtedly positive due to the shaping of the system to provide cyber security as some kind of complete and organised mechanism. It is also important to shape values and influence the perspective from which young people view today's reality.

However, the disadvantage of such a policy may be the lengthiness of the process itself. Thus, while the system developed may be an answer to future ceberconflicts, the solutions to the Ukrainian-Russian conflict must be found elsewhere.

---

712 'ECCC to be present at the CYBERSEC Forum & Expo 2023, 21-22 June in Katowice' (*ECCC*, 13 June 2023) <https://cybersecurity-centre.europa.eu/news/eccc-be-present-cybersec-forum-expo-2023-21-22-june-katowice-2023-06-13_en> accessed 16 December 2023.

713 'About Leitmotif 2023' (*CyberSec*) <https://cybersecforum.eu/pl/cybersec-forum-expo-2023/> accessed 16 December 2023.

714 Korsak E, 'Polska rozwija cyberobronę' (*Polska Zbrojna*, 22 June 2023) <https://polska-zbrojna.pl/home/articleshow/39825?t=Polska-rozwija-cyberobrone> accessed 16 December 2023.

Conclusion

'The internet is being used not only to commit cyber attacks, but also to shape a new reality. (…) The spread of disinformation through cyberspace, particularly using social media, makes it possible to manipulate society on a mass scale.'[715]

Taking into consideration the example of the 15 February 2022 attack by Russia, the position expressed above can easily be confirmed. The primary goal of those carrying out a cyber attack is often not the acquisition of data itself, but to confuse the public, sow panic and create an atmosphere of intimidation. The idea is consequently to deprive citizens, as well as authorities, of a sense of control. The hybrid war is, therefore, really not so much an information war as it is primarily a psychological war. This conclusion seems to be confirmed by Sven Herpig who has been already quoted above. He claimed that cyber operations have become part of modern psychological war these days and the aim of themwas to alarm the population and break the willingness to resist.[716]

The second conclusion relating directly to the law, which is the answer to the question posed in the introduction about the state of the contemporary legal system, is that there are clear gaps in the law in terms of the regulation needed to address the problem of hybrid war and cyber security breaches. Indeed, the existing solutions appear to be incomplete and insufficient, and some remain so ambiguous to the doctrine that the legitimacy of their application to cyber-conflicts is questioned.

[715] Gardocki S, Wrona J, 'Russia's use of cyberspace in hybrid conflicts in the light of Russian cyber security policy' (2020) 2(38) *Colloquium* 33.

[716] Taube F, 'Wojna w Ukrainie. Szczególna rola cyberataków' (*DW*, 1 March 2022) <https://www.dw.com/pl/wojna-w-ukrainie-szczeg%C3%B3lna-rola-cyberatak%C3%B3w/a-60957901> accessed 16 December 2023.

6.2 Securing the Post-Pandemic World: What is a Cure for Infodemia?

By ***Michał Byczyński*** (University of Lodz)

Introduction

In the midst of the COVID-19 pandemic, an avalanche of unfounded claims has swiftly inundated social media platforms. These assertions encompass a wide array of untruths, including dubious allegations regarding the virus's origins, deceptive health-related information, and rumors designed to sow uncertainty about the safety and efficacy of vaccines.

The Vice-President of the European Commission for Values and Transparency has formulated the term "coronavirus infodemic" to describe this disturbing scenario, underlining how false or misleading information has caused serious damage to public health, cast a shadow on the economy and undermined the response of government authorities.

The creation of deceptive information, which may closely resemble traditional news content in appearance but lacks the same organizational principles and motives, has wielded an alarmingly disproportionate influence over the way individuals perceive real-world events and make political choices. This phenomenon can be primarily attributed to the wide-reaching manipulability of information across the broader internet landscape, particularly on social media platforms. The adverse consequences are not confined to any specific category of false or misleading information, often termed "misinformation", but are of greatest concern when such information is deliberately generated and disseminated with the explicit intent to deceive the public, a practice known as "disinformation". This is deeply disconcerting because the ability to exploit online communication channels has evolved into a potent instrument for information warfare and foreign interference, enabling the manipulation of information for deceptive purposes.

This article investigates the multifaceted challenge of infodemia[717] encompassing the role of misinformation in eroding human rights, the potential solutions offered by international law, and strategies for promoting reliable information (part 2, 3, 4 and 5). Additionally, it explores the application of AI and machine learning techniques in identifying and countering infodemia (part 6).

The research methodology involves a thorough review and analysis of existing literature, reports, and documents pertaining to the topic of infodemia, with a focus on the COVID-19 pandemic and misinformation surrounding it. Key sources include academic publications, reports from international organizations, governmental statements,

[717] For the purposes of this article *infodemia* (synonymous with '*infodemic*') should be understood as a state characterized by the pervasive influence of misinformation and disinformation on individuals' lives, resulting in a harmful impact. This state often involves the rampant spread of falsehoods, manipulation, and misleading narratives, affecting various aspects of society, from public health to human rights and international relations. Misinformation and disinformation should be perceived as causes of infodemia in this context.

and expert opinions. By adopting a multi-faceted methodology, this article provides a holistic examination of the infodemia issue, offering insights and recommendations based on both scholarly research and real-world experiences.

1. Infodemia: The Proliferation of Falsehoods

At the outset of the COVID-19 pandemic in February 2020, the Director General of the World Health Organization (WHO), Tedros Adhanom Ghebreyesus, sounded an early warning: "we're not just fighting an epidemic; we're fighting an infodemic. Fake news spreads faster and more easily than this virus and is just as dangerous".

The WHO defines an infodemic as "too much information including false or misleading information in digital and physical environments during a disease outbreak. It causes confusion and risk-taking behaviours that can harm health. It also leads to mistrust in health authorities and undermines the public health response".[718] The rise of social media and the internet has exacerbated the infodemic, intertwining misinformation with the pandemic's dynamics. To counteract this, the WHO advocates for infodemic management based on risk- and evidence-based analysis, offering credible health information, and building resilience against misinformation or disinformation.[719]

To address the infodemic, the WHO and experts advocate for information hygiene to promote responsible individual behavior. Information hygiene, meaning elimination of misinformation and disinformation from circulation, is considered crucial to prevent the spread of infodemia. Building individual resilience against infodemic is promoted as a way to build societal resilience against disinformation and the pandemic itself.[720]

Various initiatives to counter COVID-19 misinformation have emerged, with a focus on increasing trust in scientific evidence, promoting vaccine positivity, and fact--checking to debunk myths.[721] These initiatives involve governments, civil society, and international organizations, emphasizing information hygiene, media literacy, and fact--checking. Some of them engage artificial intelligence-based technologies pointed at detecting and eliminating false information from online circulation.[722]

2. Infodemia's Assault on Human Rights

Infodemia endangers a number of human rights. As misinformation and disinformation frequently aims to damage the victims' reputation[723] potential violations of the

[718] World Health Organization, 'Infodemic', (2022) <https://www.who.int/health-topics/infodemic#tab=tab_1> accessed 10 October 2023.

[719] Ibid.

[720] See, World Health Organization, 'WHO policy brief: COVID-19 infodemic management', (2022), <https://www.who.int/publications-detail-redirect/WHO-2019-nCoV-Policy_Brief-Infodemic-2022.1> accessed 10 October 2023.

[721] Cuan-Baltazar JY, Muñoz-Perez MJ, Robledo-Vega C, Pérez-Zepeda MF, and Soto-Vega E, 'Misinformation of COVID-19 on the Internet: Infodemiology Study' (2020) 6(2) *JMIR Public Health Surveill* 8444.

[722] Cueva E, Ee G, Iyer A, Pereira A, Roseman A and Martinez D, 'Detecting Fake News on Twitter Using Machine Learning Models', Paper presented at the (2020) *IEEE MIT Undergraduate Research Technology Conference (URTC),* Cambridge, MA, USA, pp. 1-5.

[723] Hameleers M, van den Meer T and Vliegenhart R, 'Civilized Truths, Hateful Lies? Incivility and Hate

right to privacy (Article 17 of the International Covenant on Civil and Political Rights [ICCPR]) must be considered. Additionally, in certain instances, the dissemination of disinformation can encroach upon the fundamental principle of non-discrimination. This occurs when false or misleading information is deliberately aimed at specific societal groups, such as migrants or particular communities, with the malicious intent of sparking violence, nurturing discrimination, or inciting hostility. In other words, disinformation doesn't merely represent a passive spread of falsehoods; it can be weaponized as a tool to actively perpetuate prejudices and divisions within society.

In some circumstances, hate speech-containing misinformation could potentially be considered a violation of Article 20(2) ICCPR. One could even contend that war propaganda violates the right to life of individuals guaranteed by Article 6 ICCPR by fanning the flames of hatred and violence, as is the case with Russian disinformation regarding Ukraine.[724] Disinformation may also infringe the freedom of opinion enshrined in Article 19(1) ICCPR.[725] It appears that users can be effectively and widely manipulated thanks to contemporary technologies. Regarding this, spreading false information in violation of Article 19(1) ICCPR may also constitute a violation of Article 25 ICCPR, which upholds the right to free and fair elections.[726]

States who produce and disseminate misinformation may be violating the targeted population's right to health, as stipulated in Article 12 of the International Covenant on Economic, Social, and Cultural Rights (ICESCR), for example by disseminating false information regarding the effectiveness or safety of vaccines.[727] Research reveals that a significant 40% of health-related news circulated online is fabricated, and vaccines are a major area of concern in this context.[728] While the decision to vaccinate children remains a matter of personal choice in numerous countries, health authorities emphasize that opting not to vaccinate children can have detrimental consequences for public health. For instance, recent dissemination of false information claiming a link between the measles, mumps, and rubella vaccine and autism led to the declaration of multiple public health emergencies, as reported by the UN.[729] Misleading information pertaining to healthcare and disease prevention, particularly falsehoods concerning vaccine-related risks, has the potential to dissuade individuals from making informed healthcare choices

Speech in False Information - Evidence from Fact-Checked Statements in the US.' (2021) 25(11) *Information, Communication & Society* 1596, p. 14.

[724] Human Rights Committee, 'General Comment No. 36 on Article 6 of the International Covenant on Civil and Political Rights, on the Right to Life', Adopted by the Committee at its 124th session (8 October to 2 November 2018). UN Doc. CCPR/C/GC/36, (2018), para 59.

[725] Alegre S, 'Rethinking Freedom of Thought for the 21st Century.' (2017) 3 *European Human Rights Law Review* 221, p. 225.

[726] Zerbe Y, 'Cyber-Enabled International State-Sponsored Disinformation Operations and the Role of International Law' (2023) 33 *SRIEL* 49, p. 62.

[727] Human Rights Council, 'Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression', UN Doc. A/HRC/44/49 (23 April 2020), passim.

[728] Waszak PM, Kasprzycka-Waszak W and Kubanek A, 'The Spread of Medical Fake News in Social Media – The Pilot Quantitative Study' (2018) 7(2) *Health Policy and Technology* 115, pp. 115–118.

[729] See, Swire-Thompson B, Lazer D, 'Public Health and Online Misinformation: Challenges and Recommendations' (2020) 41(1) *Annual Review of Public Health* 433, pp. 433–451.

that safeguard their well-being. This, in turn, places both the affected individuals and the broader community at an increased risk. An example of this phenomenon was visible during the COVID-19 pandemic, where the proliferation of health-related misinformation and disinformation contributed to vaccine hesitancy, thereby undermining public health efforts across the globe.

3. The Role of International Law in Combating Infodemia

Considering the global harm caused by State-influenced disinformation, it makes sense to look to international law, which main goal is to guarantee the peaceful coexistence of states, for solutions to counteract infodemia. Noteworthy, the Human Rights Council has affirmed through various resolutions that international human rights law (IHRL) applies to the internet and that human rights must therefore be respected in cyberspace as well.[730]

The exercise of IHRL is still mostly restricted to national borders, or at the very least, territorial control, due to its state-centered orientation.[731] Therefore, as a result of ratifying international human rights treaties, states owe both positive and negative human rights duties to the individuals within their borders. Nonetheless, the concept of *effective control* mandates that states that possess territorial authority over other states guarantee the preservation of human rights within that area.[732] When there is no territorial control, there are no duties owing to the people who reside in other States.[733] While there is a continuous discourse in academia regarding the *transnationalization* of international human rights law, states and international courts are hesitant to extend the extraterritorial scope of IHRL due to the present State-centered approach's incapacity to encompass globalized phenomena like migration, transboundary environmental harm, or even international disinformation campaigns.[734]

When considering the role of international law in combating infodemia, the principle of non-intervention in the internal affairs of other states must be acknowledged.[735] The principle is considered "one of the fundamental duties of the State"[736] and has been acknowledged as an integral part of customary international law[737] by the International

[730] Human Rights Council, 'Promotion and Protection of All Human Rights, Civil, Political, Economic, Social and Cultural Rights, Including the Right to Development', A/HRC/47/L.22, (7 July 2021), p. 3.

[731] Mishra A, 'State-Centric Approach to Human Rights: Exploring Human Obligations' (2019) 32 *Rev Quebecoise de Droit Int'l* 49, p. 57.

[732] ECtHR, *Al-Skeini v. United Kingdom*, Appl. No. 55721/07, Judgment (7 July 2011), paras 138–140.

[733] Milanovic M, *Extraterritorial Application of Human Rights Treaties* (OUP, 2011), p. 210.

[734] See, supra (n 726), p. 62.

[735] Ibid.

[736] Kunig P, 'Intervention, Prohibition of', *Max Planck Encyclopedia of Public International Law* <https://tinyurl.com/mw8nzf98> accessed 3 October 2023, para 7.

[737] ICJ, *Case Concerning Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America)*, Judgment [1986] ICJ Rep 1986, para 202; see also, ICJ, *Corfu Channel (United Kingdom of Great Britain and Northern Ireland v Albania)* Judgment [1949] ICJ Rep 4.

Court of Justice (ICJ). This principle emanates from the concept of sovereignty outlined in Article 2(1) of the UN Charter.[738]

While it is evident that states interact with one another and exert influence, whether directly or indirectly, there are specific forms of intervention in the internal affairs of other states that have been formally proscribed by international law through the UN Charter and resolutions of the United Nations General Assembly (UNGA).[739] Such interactions are clearly visible during the infodemic, where information flows from one country to another, sometimes being disseminated at the initiative of governments, prompting the need for global coordination and regulation to combat misinformation on a wide scale.

UNGA Resolution 2625 (XXV) of 1970, known as the Friendly Relations Declaration, played a pivotal role in delineating the limits of intervention. It asserted that no state possesses "the right to intervene, directly or indirectly, for any reason whatsoever, in the internal or external affairs of any other state".[740] Notably, the International Group of Experts (IGE), responsible for creating the Tallinn Manual, has affirmed that the principle of non--intervention extends to the realm of cyberspace.[741]

Therefore, any global legal efforts by the international community to combat infodemia must carefully account for the unique characteristics and intricacies of international law in this context. Moreover, the multifaceted nature of infodemia, which encompasses not only the dissemination of false information but also the manipulation of public opinion, requires a holistic approach that involves not only legal mechanisms but also international cooperation in the realms of media literacy, technology regulation, and diplomatic efforts. This comprehensive strategy can help address the complex challenges posed by infodemia and its impact on global society.

4. Promoting Reliable Information and an Enabling Environment

Recognizing the distinct character of disinformation, the global community as a whole has taken a first and important step with HRC Resolution 49/21. According to Resolution 49/21 governments ought to make an effort to draft a comprehensive, legally binding agreement that prohibits international State-sponsored disinformation.[742] Such a convention ought to clearly indicate that any intentional attempt to use disinformation to control and harm a population of a foreign country is illegal interference in the sovereign state's territory.

---

738 UN, Charter of the United Nations, adopted on 24 October 1945, 1 UNTS 16, Article 2(1) UNC.

739 UNGA, Res 2131 (XX), 'Declaration on the Inadmissibility of Intervention and Interference in the Internal Affairs of States' UN Doc. A/RES/36/103 (1981).

740 UNGA, Res 2625 (XXV), Declaration on Principles of International Law Concerning Friendly Relations and Co-operation among States in Accordance with the Charter of the United Nations, (1970) (Friendly Relations Declaration); ICJ, *Case concerning armed activities on the territory of the Congo (DRC v. Uganda)*, Judgment [2005] ICJ Rep 168, para 155–65.

741 Schmitt M, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (CUP, 2017), p. 312.

742 Zhao W, 'Cyber Disinformation Operations (CDOs) and a New Paradigm of Non-Intervention' (2020) 27 *U.C. Davis Journal of International Law & Policy* 35, p. 51.

However, false and misleading information cannot be easily censored or simply expunged, particularly in the age of social media and messaging apps. Restricting information and the free expression of opinions and ideas through censorship, internet shutdowns, and persecution of human rights defenders or journalists, are ineffective measures that do not tackle the root causes of why the public remains vulnerable to misinformation. Restrictions on the right to freedom of expression that impose blanket prohibitions on the dissemination of information, including those based on vague and ambiguous concepts such as "false news" or "spreading misinformation", are surely incompatible with international human rights law.[743]

As stated by the UN Human Rights Committee, international law does not permit general prohibitions of expressions of an erroneous opinion or an incorrect interpretation of events.[744] Legislation prohibiting and criminalizing "fake news" also risks having a chilling effect on the general population and the media, leading to self-censorship out of fear of reprisals. As noted by the UN Special Rapporteur on the right to freedom of expression, such limitations often appear not to be imposed for the legitimate purpose of promoting accurate information but in order to suppress relevant information uncomfortable for the government or to use the situation as a pretext to crack down on opposition politicians, critical media outlets or human rights defenders.[745]

As emphasized by regional and international experts on the right to freedom of expression, public officials should take care to ensure that they disseminate reliable and trustworthy information, including about matters of public interest.[746] States are required to step up their efforts to ensure that they disseminate reliable, accessible, evidence--based and trustworthy information, which is crucial to counter false and misleading information.[747] States also have an obligation to ensure an enabling environment for freedom of expression, including by promoting a free, independent and diverse communications environment which is a key means of addressing misinformation and propaganda.[748] In 2017 international and regional experts on freedom of expression laid down a series of obligations and general principles for States to follow in order to combat misinformation.[749]

---

[743] Human Rights Council, 'Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression', UN Doc. A/HRC/44/49 (23 April 2020), para 49.

[744] Human Rights Committee, 'General Comment No. 34, Article 19: Freedoms of opinion and expression', UN Doc. CCPR/C/GC/34, (2011), para 49.

[745] Human Rights Council, 'Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression', UN Doc. A/HRC/44/49 (23 April 2020), para 47.

[746] Human Rights Council, 'Report of the Special Rapporteur on Freedom of Opinion and Expression, OSCE Representative on Freedom of the Media, Special Rapporteur on Freedom of Expression of the Inter-American Commission on Human Rights, and the Special Rapporteur on Freedom of Expression and Access to Information of the African Commission on Human and Peoples' Rights, Joint Declaration on Freedom of Expression and "Fake News", Disinformation, and Propaganda', (3 March 2017), para 2.d.

[747] Ibid.

[748] Ibid., para 3.a.

[749] Human Rights Council, 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression', Irene Khan Disinformation and Freedom of Opinion and Expression. UN Doc. A/HRC/47/25, (13 April 2021).

Moreover, UNESCO has encouraged States to take steps to understand and monitor the reasons behind and the sources of misinformation and disinformation[750]. Among other relevant measures, UNESCO has recommended governments to create an environment in which it is possible to conduct careful fact-checking and debunking of false or misleading information; providing government support and funding for quality and public interest journalism and counter disinformation campaigns on media and social media platforms; supporting the target audiences of disinformation campaigns; strengthening ethical standards in reporting; educating the public and journalists and empowering them to differentiate between quality news and unreliable information. States also need to ensure people can effectively exercise their right to freedom of expression without discrimination, including by protecting individuals against abuses by non-state actors.[751]

States should avoid delegating responsibility to companies as adjudicators of content, which empowers corporate judgment over human rights values to the detriment of users.[752] In this regard, states must uphold the principle that intermediaries should not be required to substantively evaluate the legality of third-party content, in line with the Manila Principles on Intermediary Liability.[753] However, companies involved in moderating online content must uphold their human rights responsibilities, including by carrying out human rights due diligence and ensuring greater transparency regarding, and oversight of, content moderation practices and policies and the algorithmic systems underpinning their platforms to ensure that human rights are respected in practice.[754]

5. Leveraging AI and Machine Learning

According to Lazarotto two essential strategies for preventing the spread of misinformation are fact-checking and content control.[755] Despite their appearance, they are not the same. Content moderation is a function of social media platforms and is governed by their policies. Its goal is to identify and delete entries that contain prohibited content.[756] However, the goal of fact-checking is to identify which information about a subject is accurate and which information was presented in error.[757]

---

[750] See, UNESCO, 'Disinfodemic: Deciphering Covid-19 Disinformation' (2020) <en.unesco.org/sites/default/files/disinfodemic_deciphering_covid19_disinformation.pdf> accessed 20 October 2023.

[751] Human Rights Committee, 'General Comment No. 34, Article 19: Freedoms of opinion and expression', UN Doc. CCPR/C/GC/34, (2011), para 7.

[752] Human Rights Council, 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression', UN Doc. A/HRC/38/35 (6 April 2018).

[753] 'Manila Principles on Intermediary Liability' <https://manilaprinciples.org/principles.html> accessed on 20 October 2023.

[754] See, supra (n 752).

[755] Lazarotto B, 'The Impact of Disinformation During the COVID-19 Pandemic and Its Regulation by the EU' (2020) 6 *EU Law Journal* 2, p. 31.

[756] Habersaat KB, Betsch C, Danchin M, Sunstein CR, Böhm R, Falk A, Brewer NT, Omer SB, Scherzer M, Sah S, 'Ten considerations for effectively managing the COVID-19 transition.' (2020) 4 *Nature Human Behaviour* 677, pp. 677–687.

[757] Barrett PM, *Who Moderates Social Media Giants? A Call to End Outsourcing* (NYU CBHR, 2020), p. 23.

Journalists and scientists, for example, are human domain specialists who can identify COVID-19 fake news[758] however with so much information flooding the internet every day, it becomes hard and resource-intensive for people to identify bogus news. AI technologies can detect fake news about the disease by applying machine-learning techniques for mining social media information, tracking down words that are sensational or alarming, and identifying which online sources are deemed authoritative for fighting infodemia.

Machine learning methods are becoming more and more popular since they can automatically assess the veracity of COVID-19 news from internet channels.[759] Different controlled methods for learning, such as the random forest[760], logistic regression[761] or support vector machine[762], were adopted to train prediction models for detecting COVID-19 fake news. Extraction of machine-understandable information from the news items is crucial for machine learning-based COVID-19 false news predictions. [763] It is possible to identify COVID-19 fake news using linguistic and sentiment traits, according to recent research. For instance, determining the writing style of fake news can be done by counting the quantity of uppercase characters.[764]

Conclusion

The intricate and widespread nature of infodemia stemming from hostile information operations presents a substantial quandary to national security. It stands as a formidable challenge that is likely to test the efficacy of international law in its capacity to shield against such threats. Consequently, international community is grappling with the formulation of regulatory strategies to combat the propagation of erroneous or deceptive information, seeking to navigate the intricate landscape of this modern information warfare. This complex landscape underscores the necessity for a multifaceted response at both national and international levels to protect the integrity of information and the stability of societies in an interconnected world.

Efforts to combat infodemia require a multi-pronged approach that acknowledges the unique challenges posed by digital communication. International law, which traditionally operates within state borders, must adapt to encompass the globalized nature of information dissemination. Promoting reliable information and creating an enabling

[758] Tashtoush Y, Alrababah B, Darwish O, Maabreh M and Alsaedi N, 'A Deep Learning Framework for Detection of COVID-19 Fake News on Social Media Platforms' (2022) 7 *Data* 5, p. 2.

[759] Varma R, Verma Y, Vijayvargiya P and Churi PP, 'A systematik survey on deep learning and machine learning approaches of fake news detection in the pre-and post-COVID-19 pandemic.' (2021) 14 *International Journal of Intelligent Computing and Cybernetics* 617, pp. 617–646.

[760] Khan S, Hakak S, Deepa N, Prabadevi B, Dev K, Trelova S, 'Detecting COVID-19-Related Fake News Using Feature Extraction' (2022) 9 *Frontiers in Public Health* 788074, p. 9.

[761] Ibid.

[762] Abdelminaam DS, Ismail FH, Taha M, Taha A, Houssein EH, Nabil A, 'CoAID-DEEP: An Optimized Intelligent Framework for Automated Detecting COVID-19 Misleading Information on Twitter.' (2021) *IEEE Access* 9, pp. 27840–27867.

[763] See, supra (n 760).

[764] Al-Rakhami MS and Al-Amri AM, 'Lies Kill, Facts Save: Detecting COVID-19 Misinformation in Twitter' (2020) 8 *IEEE Access* 155961, pp. 155961–155970.

environment for freedom of expression are essential components of the strategy to counteract infodemia. While restrictions on the free expression of ideas may seem tempting, they often lead to unintended consequences, including self-censorship and the suppression of vital information.

The utilization of AI and machine learning technologies holds promise in identifying and countering misinformation. Fact-checking and content control, powered by these tools, provide valuable means of distinguishing between accurate information and erroneous claims, particularly in the context of public health crises like the COVID-19 pandemic.

CHAPTER VII

HUMAN RIGHTS

7.1 Digital Agriculture: Safeguarding Human Rights through Responsible Research and Innovation

By ***Foto Pappa*** (Sant' Anna School of Advanced Studies)

Introduction

Digital agriculture is a fast-growing sector, which encompasses the use of technology such as robots, drones, artificial intelligence (AI) and Internet of Things (IoT) in agriculture. Proponents of the introduction of digital agriculture have underlined its benefits, including improved productivity and sustainability. The way in which this would happen is through the precise application of inputs such as pesticides and fertilizers, as well as irrigation. The latter could be automatized, but it is also possible to provide individualized actionable advice to the farmer through the relevant app. To elaborate, the technology is synthesizing historical data as well as data provided by the farm (collected for example from sensors on the ground or from drones flying over the farm) in order to predict the ideal timing and quantity for example of pesticide application.

However, digital agriculture has also garnered criticism, because of the unequal power relations between digital agriculture companies and farmers, as well as the treatment of farm data. Among the risks that have been identified are market concentration-with the ensuing exacerbation of inequalities- as well as issues related to the role of the farmer, who will be more dependent on technology and runs the risk of being disconnected from the land and experimental/tacit knowledge.

Given that more and more countries are introducing digital agriculture policies or are collaborating with digital agriculture companies, more attention should be paid to the way this technology is developed and introduced. In this submission, I will be attempting to delineate what an approach that would be in compliance with human rights obligations of states -particularly the human right to science- using the paradigm of responsible research and innovation. I will be exploring what the benefits of a technology development and introduction would be, if they comply with the approach of responsible research and innovation, focusing on the benefits this could offer for digital agriculture.

1. The Human Right to Science: A safeguard and an asset for digital agriculture?

The human right to science is contained in Article 15 (1) (b) of the International Covenant on Economic Social and Cultural Rights (ICESCR) as the right of everyone "to participate in and to enjoy the benefits of scientific progress and its applications".[765] General comment (GC) 25 also sets forth that states should take measures to ensure that

[765] International Covenant on Economic, Social and Cultural Rights (adopted 16 December 1966, entered into force 3 January 1976) 993 UNTS 3, Art. 15, para 1 (b).

the needs of peasants are incorporated in agricultural research and development and that peasants participate in the determination of priorities and undertaking of research and development, with respect given to their cultures and their experience.[766]

According to the Committee on Economic Social and Cultural Rights (CESCR), the precautionary principle is also of importance when talking about "risks involved in particular scientific processes and its applications". If there is not full scientific certainty, "when an action or policy may lead to unacceptable harm to the public or the environment, actions will be taken to avoid or diminish that harm".[767] According to the classification of the CESCR, unacceptable harm encompasses the harm to humans or the environment that is: "(a) threatening to human life or health; (b) serious and effectively irreversible; (c) inequitable to present or future generations; or (d) imposed without adequate consideration of the human rights of those affected".[768] Thus, according to the CESCR, tools that are useful in identifying potential risks are technological and human rights impact assessments.[769]

It is pertinent to note a criticism that has been put forth regarding the abovementioned reiteration of the precautionary principle within GC 25. According to scholar Samantha Besson, the GC 25 defines the acceptability of the harm while referring to the human rights of those affected. Thus, it errs by considering these rights as external to the right. It is her opinion that anticipation duties should be framed under the human right to science itself-because they are inherent in the protection of the right to science-and not under duties arising under other human rights.[770]

Regarding the risks, states would be complying with an implicit obligation contained within the right to science. It has been argued that states are also under an obligation to protect from the negative effects that science (and technology) might have on human rights enjoyment.[771] An interpretation *a contrario* to the wording of Article 15 could be supporting this argument, or in the alternative, a systematic and teleological interpretation that considers the entirety of both Covenants.[772]

To demonstrate, the CESCR both in its Guidelines on Reporting by states,[773] as well as its GC 25 has argued that the right to science could be interpreted as encompassing

---

[766] CESCR, 'General comment No. 25 on science and economic, social and cultural rights (article 15 (1) (b), (2), (3) and (4) of the International Covenant on Economic, Social and Cultural Rights)' (30 April 2020) UN Doc E/C.12/GC/25, para 65.

[767] Ibid., para 56.

[768] Ibid.

[769] Ibid.

[770] Besson S, 'Anticipation under the human right to science: concepts, stakes and specificities' (2024) 28(3) *The International Journal of Human Rights* 293, p. 299.

[771] Mazibrada A, 'Is there a Right to be Protected from the Adverse Effects of Scientific Progress and its Applications?' (*EJIL: Talk!*, 29 November 2022) <https://www.ejiltalk.org/is-there-a-right-to-be-protected-from-the-adverse-effects-of-scientific-progress-and-its-applications/> accessed 29 October 2023.

[772] Ibid.

[773] CESCR, 'Guidelines on Treaty-Specific Documents to be Submitted by States Parties under Articles 16 And 17 of the International Covenant on Economic, Social and Cultural Rights (24 March 2009)' UN Doc E/C.12/2008/2, para 70 (b).

a state obligation to prevent from the risks, harms and effects of science that would be contrary to the enjoyment of human rights.

Conversely, it has been argued that the duty of anticipation contained within the right to science is twofold. It does indeed include a duty to anticipate and protect from the risks of harm, but at the same time it contains a duty to identify the opportunities for the benefits of science and its applications.[774]

It is noteworthy to consider how this can be applied to digital agriculture. First, we need to establish that digital agriculture falls under the protection guaranteed by the right to science. Digital agriculture may fall under the term "benefits" in the iteration of the right: "everyone has a right "to enjoy the benefits of scientific progress and its applications". According to the CESCR, "benefits" include both "material results of the applications of scientific research"[775] but also to the derivatives of scientific activity i.e. scientific knowledge and information.[776] Thus, both the hardware and software that are used in the context of digital agriculture are covered by the term "benefits of scientific progress and its applications".

Moreover, under the obligation to fulfil the right to science, and according to the CESCR, states are under the obligation to remove hurdles that persons may face in accessing the benefits of science.[777] This merits our attention as it would mean that additionally, states have an important role to play with regard to the hurdles that farmers may face in accessing digital agriculture technology. These include for example the digital divide, with access to internet, smartphones and other useful equipment not being available to all, especially not in the less developed countries.[778] Furthermore, hurdles also include the issue of digital literacy of the population, with the rural poor being at a disadvantage.[779] Thus, in order to comply with their obligations under the right to science, states will have to aim to also address the underlying prerequisites that will affect the access to digital agriculture technology since accessibility is part of the right to science, with the CESCR underlining that "scientific progress and its applications should be accessible for all persons, without discrimination".[780] This is particularly important given the power imbalances and inequalities that have been mentioned in relation to the diffusion of digital agriculture, which has so far focused on industrialized big farms.

Concludingly, our takeaways from an analysis of the human right to science state obligations should be that it is for the states to uptake measures to protect from the negative effects that digital agriculture might have on the enjoyment of human rights.

---

[774] Müller A, 'Anticipation under the human right to science (HRS): sketching the public institutional framework. The example of scientific responses to the appearance of SARS-CoV-2' (2024) 28(3) *The International Journal of Human Rights* 439, p. 445.

[775] GC 25 (n 766), para 8.

[776] Ibid.

[777] GC 25 (n 766), para 47.

[778] Ye L and Yang H, 'From Digital Divide to Social Inclusion: A Tale of Mobile Platform Empowerment in Rural Areas' (2020) 12 *Sustainability* 1, p. 1.

[779] Hackfort S, 'Patterns of Inequalities in Digital Agriculture: A Systematic Literature Review' (2021) 13 *Sustainability* 1, p. 6.

[780] GC 25 (n 766), para 17.

As it will be shown below, one of the possible avenues in taking a proactive approach would be the encouragement of responsible research and innovation. The latter has received growing attention, with business ethics professor and consultant Michael A. Santoro warning technology companies that if they don't stay ahead of responsible innovation, 'they risk losing their competitive edge'.[781]

2. The application of Responsible Research and Innovation to digital agriculture

The current model of innovation has been based on technological and commercialized innovation.[782] Within this model, the knowledge of farmers and the exchange of this knowledge amongst themselves has been underestimated.[783] Specifically, the model of transfer-of-technology which entails the creation of knowledge and its dissemination by experts has increasingly been criticized for the impacts it has had, but also for ignoring the importance of farmer knowledge and their peer-to-peer transfer of that knowledge.[784] In contrast, the UN Secretary General in a Report in 2021, underlined that the national assessments of technology interventions should identify the "needs and demands of small-scale producers and vulnerable groups and incorporate them into the design and application of agricultural technologies".[785] He also recommended an active involvement in "decision-making on research, development and innovation" for small-scale producers, including women, young people and indigenous peoples.[786]

However, currently there is a prevalence of private development of agricultural innovations. To illustrate, in a 2023 Report by the Food and Agriculture Organization (FAO), it was found that private investments in research and development for agriculture are increasing faster than public sector investments. The same report underlined the need to increase public research investments, because they can prioritize goals and needs such as environmental protection and sustainability over economic profit, which is not necessarily the case for private investments.[787]

In light of the above, it is important for digital agriculture technology to be designed while taking the needs and priorities of the groups affected into consideration and also in an attempt to serve society at large. The need for designing technology while having in mind the needs of the society is reflected in the discourse on Responsible

[781] Santoro M, 'A Regulatory Tsunami is Coming to Silicon Valley: Tech Companies Must Adopt Responsible Innovation or Risk Losing Their Competitive Edge' (*Cambridge Core Blog*, 9 June 2023) <https://www.cambridge.org/core/blog/2023/06/09/a-regulatory-tsunami-is-coming-to-silicon-valley-tech-companies-must-adopt-responsible-innovation-or-risk-losing-their-competitive-edge/> accessed 29 October 2023.

[782] El Bilali H, 'Relation between Innovation and Sustainability in the Agro-Food System' (2018) 30 *Italian Journal of Food Science* 200, p. 212.

[783] Ibid.

[784] Jackson-Smith D and Veisi H, 'A Typology to Guide Design and Assessment of Participatory Farming Research Projects' (2023) 5 *Socio-Ecological Practice Research* 159, p. 159.

[785] UNGA, 'Report of the Secretary General on Agriculture technology for sustainable development: leaving no one behind', UN Doc A/76/227 (2021), para 80.

[786] Ibid.

[787] Ruane J and Ramasamy S, 'Global investments in agricultural research: Where are we and where are we going?' (*FAO*, 2023) <https://www.fao.org/3/cc6971en/cc6971en.pdf> accessed 29 October 2023.

Research and Innovation (RRI). According to this approach, technology should be designed in line with societal needs.[788] Scholars have examined the application of RRI for technology in different sectors, including urban transport and medical applications, aiming to understand the benefits of an RRI approach.[789]

As part of the four axes of RRI, anticipation aims at identifying the impacts of a certain technology, including the minimization of the negative impacts.[790] In the case of digital agriculture, anticipation could encompass all kinds of impacts: "on-farm, across farming landscapes, throughout the food chain, as well as considering effects on rural communities and publics as a whole".[791] Another element of RRI is inclusion, which encompasses the engagement of different actors in the innovation process.[792] Moreover, the axis of reflexivity entails that researchers need to be aware of their preconceived ideas and their motivations, and actively engage in an interaction with other actors. Reflexivity is essentially the awareness that a novel technology may bring opportunities, but it could also create or worsen existent problems.[793] Lastly, responsiveness entails the shift in the trajectory of the research/innovation as a response to the inputs received through the interaction with the different actors.[794]

3. Farmers' participation in RRI in digital agriculture

As it was demonstrated, RRI encompasses anticipation, which as was highlighted above is part of the obligations incumbent upon states under the human right to science. As part of the inclusion element of RRI, regarding digital agriculture, a recent study categorized the stakeholders as micro-level, meso-level and macro-level. Farmers are part of the first category, and according to the writers of the study, even though they are very often referred to as catalytical for digital agriculture development and adoption, in practice they receive much less attention.[795] Thus, a model built on participation and knowledge sharing would be apt to agricultural innovation.[796]

---

[788] Gremmen B, Blok V and Bovenkerk B, 'Responsible Innovation for Life: Five Challenges Agriculture Offers for Responsible Innovation in Agriculture and Food, and the Necessity of an Ethics of Innovation' (2019) 32 *Journal of Agricultural and Environmental Ethics* 673, p. 674.

[789] Li W et al, 'The Making of Responsible Innovation and Technology: An Overview and Framework' (2023) 6 *Smart Cities* 1996, pp. 1997-99.

[790] Jakku E et al. 'Reflecting on Opportunities and Challenges Regarding Implementation of Responsible Digital Agri-Technology Innovation' (2022) 62 *Sociologia Ruralis* 363, p. 370.

[791] Rose DC and Chilvers J, 'Agriculture 4.0: Broadening Responsible Innovation in an Era of Smart Farming' (2018) 2 *Frontiers in Sustainable Food Systems* 1, p. 3.

[792] Stilgoe J, Owen R and Macnaghten P, 'Developing a framework for responsible innovation' (2013) 42(9) *Research Policy* 1568.

[793] Jakku E et al (n 790), p. 375.

[794] Henchion MM et al, 'Developing "Smart" Dairy Farming Responsive to Farmers and Consumer-Citizens: A Review' (2022) 12 *Animals* 1, p. 4.

[795] Ebrahimi HP, Schillo RS and Bronson K, 'Systematic Stakeholder Inclusion in Digital Agriculture: A Framework and Application to Canada' (2021) 13 *Sustainability* 1, p. 8.

[796] Molina N et al, 'Farmers' Participation in Operational Groups to Foster Innovation in the Agricultural Sector: An Italian Case Study' (2021) 13 *Sustainability* 1, p. 1.

A participatory approach thus, where farmers take part in the technology design process, is useful in many ways. In terms of policy making, it could help bridge the lag that sometimes exists between policy making and technological progress.[797] It would thus assist in anticipating the effects that could be envisaged and assist in addressing them in a proactive manner instead of reactively. A participatory approach would also be helpful in highlighting farmer's needs and priorities, and it would help incorporate their tacit knowledge within the technology.[798] If farmers are part of the testing processes as well, it could lead to a heightened trust in the technology and more farmers would adopt it.[799]

It has been argued that in relation to agricultural decision support systems (such as apps providing recommendations based on data from e.g. drones, sensors and satellites), technology developers will have to take into account elements that end-users (farmers) would want to be part of the technology. For example, they should make sure that they are using a user-friendly interface or that there is adaptability of the technology to peculiar farm situations, or the fact that maybe farmers are unwilling to turn to new farm advisors in order to use the proposed technology.[800] Participatory design could potentially also provide the benefit of the technology reaching stakeholders that it would otherwise be impossible or difficult to reach, such as older or remote rural farmers.[801]

The latter would be a very welcome advancement for many reasons. Firstly, it has been highlighted that digital agriculture is mainly benefitting large/industrial farms.[802] This is mainly due to two reasons, firstly, the barriers that small food producers face in accessing digital agriculture technology, for example due to cost[803] and lack of infrastructure such as access to internet,[804] but also because the digital agriculture paradigm is based on monocultures, which are associated with intensive/industrial agriculture.[805] To illustrate, it has been estimated that "all agricultural robots currently under commercial development require a monoculture".[806] The local needs and type of production may play an important role in the farmers' decision to adopt (or not

[797] Bronson K, 'Smart Farming: Including Rights Holders for Responsible Agricultural Innovation' (2018) 8 *Technology Innovation Management Review* 7, p. 11.

[798] Schillings J, Bennett R and Rose DC, 'Managing End-User Participation for the Adoption of Digital Livestock Technologies: Expectations, Performance, Relationships, and Support' (2024) 30(2) *The Journal of Agricultural Education and Extension* 277, p. 279.

[799] Ibid.

[800] Gardezi M et al, 'In Pursuit of Responsible Innovation for Precision Agriculture Technologies' (2022) 9(2) *Journal of Responsible Innovation* 224, pp. 238–239.

[801] Townsend LC and Noble C, 'Variable Rate Precision Farming and Advisory Services in Scotland: Supporting Responsible Digital Innovation?' (2022) 62 *Sociologia Ruralis* 212, p. 216.

[802] Fraser A, '"You Can't Eat Data"?: Moving beyond the Misconfigured Innovations of Smart Farming' (2022) 91 *Journal of Rural Studies* 200, p. 203.

[803] Stock R and Gardezi M, 'Make Bloom and Let Wither: Biopolitics of Precision Agriculture at the Dawn of Surveillance Capitalism' (2021) 122 *Geoforum* 193, p. 196.

[804] Mehrabi Z et al, 'The Global Divide in Data-Driven Farming' (2021) 4 *Nature Sustainability* 154, p. 156.

[805] Bronson K, 'Looking through a Responsible Innovation Lens at Uneven Engagements with Digital Farming' (2019) 90–91(1) *NJAS – Wageningen Journal of Life Sciences* 1, p. 4.

[806] Reisman E, 'Sanitizing Agri-Food Tech: COVID-19 and the Politics of Expectation' (2021) 48 *Journal of Peasant Studies* 910, p. 920.

adopt) digital agriculture technologies. For example, it was found that in Switzerland the interest in digital agriculture so far has been limited, due to the small size of the farms and the chasm between technology and the local context.[807]

However, a challenge that relates to the local context, is the difficulty in scalability. Will the technology which has been developed in accordance with the needs of a small group of participants be able to be scaled and appeal to users worldwide? It has been argued that the engagement of a diverse group of participants would assist in this regard. It could allow to forecast modifications from the beginning of the design process, which could prove helpful for the scalability of the product.[808]

The local context is also of paramount importance in the context of the participatory process. For example, a study found that women in Kenya were reluctant to share their opinion in a group where the majority was male participants.[809] Thus, alternative forms of engagement that would encourage the participation of all stakeholders should be part of the participatory process. Some modes of current inclusion of farmers in research projects range include "stakeholder groups; farmer technology groups; operational groups; knowledge transfer groups; design thinking; co-creation; on-farm pilot studies; demonstration farms; farm open days; farmer conferences".[810]

Another process that has been used by agricultural providers has been the use of living labs. Living labs is a type of inclusive participation that is immersive, meaning that the users of the technology are involved in testing and co-developing technology in cooperation with researchers, practitioners, and other partners in a real-life environment.[811] Nevertheless, it needs to be ascertained that the living lab is not used only for commercial purposes such as introducing the technology to the end-user/customer but for actually achieving societal goals "such as improving democratic participation or addressing ethical concerns related to new technologies".[812]

Thus, it is important to note that there are different models of farmer participation and engagement, in terms of the level of participation, the stage of participation and the location of where this interaction takes place. For example, in terms of the stage when farmers get involved, it could be during the design process, the testing process or the diffusion process.[813] It is also worth mentioning that if the farmers have played an active role in the design and development of the technology, they would be more likely to also

---

807 Forney J and Dwiartama A, 'The Project, the Everyday, and Reflexivity in Sociotechnical Agri-Food Assemblages: Proposing a Conceptual Model of Digitalisation' (2023) 40 *Agriculture and Human Values* 441, p. 447.

808 Steinke J et al, 'Participatory Design of Digital Innovation in Agricultural Research-for-Development: Insights from Practice' (2022) 195 *Agricultural Systems* 1, p. 5.

809 Ibid., p. 7.

810 Regan Á, 'Exploring the Readiness of Publicly Funded Researchers to Practice Responsible Research and Innovation in Digital Agriculture' (2021) 8 *Journal of Responsible Innovation* 28, p. 38.

811 Berberi A et al, 'Enablers, Barriers, and Future Considerations for Living Lab Effectiveness in Environmental and Agricultural Sustainability Transitions: A Review of Studies Evaluating Living Labs' (2023) 1 *Local Environment* 1, pp. 1–2.

812 Gardezi M et al (n 800), pp. 239–240.

813 Jackson-Smith D and Veisi H (n 784), p. 164.

be involved in "ground truthing" the data that they are provided with and help improve the apps/technology.[814]

Another scepticism that has been voiced relates to co-creation in general, which sets forth that elements "such as representation, inclusive recruitment, agency in decision-making, accountability, or transparency" are not considered, running the risk of diminished opportunities for underrepresented groups.[815] Another caveat in the inclusion of farmers is the fact that the process may not be truly successful, and participation may only be "virtual" if underlying power relations and conflicting interests are not addressed.[816] It is noteworthy that there may be inherent challenges in the process of engaging technology designers with farmers. It has been highlighted that it is sometimes difficult to overcome the division between developers and users.[817] In this vein, it has been put forth that there is a need for the development of a relationship of respect between scientists/developers and farmers, so that needs and opportunities may be sufficiently addressed.[818] The role of public policymakers as in-betweeners among stakeholders has been underlined in the literature. It is argued that they could assist in creating a collaborative platform that would allow citizens to interact with other stakeholders, concerning digitalization. This in turn would allow *inter alia* a balance in the viewpoints, and the creation of synergies.[819]

The participation of diverse groups of farmers in the decision-making as well as the design of the technology could also help recalibrate the priorities of digital agriculture. For many years, the focus of agricultural research and development has been placed on staple crops such as wheat, rice, and corn, overlooking the needs of poorer producers and subsistence who grow cassava or quinoa.[820] This has also been the case with digital agriculture, with technology developers focusing on staple crops and not necessarily taking into account different farm practices such as intercropping.[821] This is also connected to the challenge that was mentioned above, with digital agriculture mainly benefiting large industrial farms which are mainly growing monocultures. The inclusion of different farmers would allow technology developers to recalibrate their priorities and appeal to farmers who are not following the monocultural model of production.

[814] Simelton E and McCampbell M, 'Do Digital Climate Services for Farmers Encourage Resilient Farming Practices? Pinpointing Gaps through the Responsible Research and Innovation Framework' (2021) 11 *Agriculture* 1, pp. 16–17.

[815] Ruess AK, Müller R and Pfotenhauer SM, 'Opportunity or Responsibility? Tracing Co-Creation in the European Policy Discourse' (2023) 50 *Science and Public Policy* 433, p. 441.

[816] McCampbell M, Schumann C and Klerkx L, 'Good Intentions in Complex Realities: Challenges for Designing Responsibly in Digital Agriculture in Low-Income Countries' (2022) 62 *Sociologia Ruralis* 279, p. 294.

[817] Lioutas ED and Charatsari C, 'Innovating Digitally: The New Texture of Practices in Agriculture 4.0' (2022) 62 *Sociologia Ruralis* 250, p. 270.

[818] Mooney P, 'What's cooking for climate change-technofixing dinner for 10 billion' (2018) 74(6) *Bulletin of the Atomic Scientists* 390, p. 395.

[819] Kukk M, Põder A and Viira A-H, 'The Role of Public Policies in the Digitalisation of the Agri-Food Sector. A Systematic Review' (2022) 94 *NJAS: Impact in Agricultural and Life Sciences* 217, p. 229.

[820] Tzachor A et al, 'Responsible Artificial Intelligence in Agriculture Requires Systemic Understanding of Risks and Externalities' (2022) 4 *Nature Machine Intelligence* 104, p. 105.

[821] Visser O, Sippel SR and Thiemann L, 'Imprecision Farming? Examining the (in)Accuracy and Risks of Digital Agriculture' (2021) 86 *Journal of Rural Studies* 623, p. 630.

However, it is not certain that all farmers will be open to the model of inclusion. Some producers of traditional and artisanal products have been skeptical of digitalization: for example, in Switzerland, "traditional cheese producer organisations (…) have banned milking robots from their production".[822] This is also connected to one of the risks of the introduction of digital agriculture, which is the loss of experiential knowledge. While farmers will be free from mundane tasks, they will also possibly be removed from day-to-day on-farm observation,[823] which could also be problematic for the transmission of traditional agricultural knowledge to future generations.

In light of the above, it was highlighted that through responsible research and innovation, it would be possible to anticipate farmers' needs but also risks of digital agriculture. This would also be in line with the exigencies of the human right to science obligations incumbent upon states. As it was highlighted in the previous section, under the human right to science, states are under the obligation to protect people from the negative effects of technology. With farmer knowledge incorporated into the design, and the needs of the local population in mind, it would be possible to design and develop digital agriculture technologies which would cater to a range of farmers, not solely industrial farms. In turn, these farmers would be more prone to "ground truth" the data and help in enhancing the technology further. Nevertheless, a participatory process would have its challenges. These include as was mentioned, considering the local context and the cultural relations, as well as the issue of scaling the product, with the issue of addressing power relations and the divide between farmers and scientists being of outmost importance. In any case, it would be useful for states in terms of policy making to adopt a more inclusive approach to technology design and development, both in terms of policy making but also in terms of complying with their human rights obligations under the human right to science.

Conclusion

In summary, in this submission, I aimed to examine digital agriculture-a new technology which is gaining more traction and attention- through an approach based on human rights obligations of states, as well as RRI. After an analysis of the human right to science, it was highlighted that states are under the obligation to facilitate the access to technology, as well as an obligation to protect from the negative impacts that science and technology might have on human rights enjoyment. In order to address the first obligation, it was demonstrated that states should introduce policies and measures that would help lift the hurdles that farmers face in accessing digital agriculture, including for example lack of internet connection and digital illiteracy.

Moreover, part of the obligation to protect from technological risks is the anticipation of such risks. For this reason, states should have in place policies that help protect their people. It was demonstrated how RRI might be a possible avenue to do so, highlighting the possible benefits that this approach could offer for the development as well as

[822] Finger R, 'Digital Innovations for Sustainable and Resilient Agricultural Systems' (2023) 50 *European Review of Agricultural Economics* 1277, p. 1294.

[823] Ingram J and Maye D, 'What Are the Implications of Digitalisation for Agricultural Knowledge?' (2020) 4 *Frontiers in Sustainable Food Systems* 1, p. 3.

diffusion of digital agriculture technologies. It was highlighted that if the needs of the interested parties, namely farmers are taken into account, then it is possible to design digital agriculture technologies that are more suitable to different types of farms. It was however also highlighted that this approach may face some challenges, including power relations between the groups involved, the agency of the actors involved in the participatory process, as well as the lack of trust that might exist. These underlying issues would have to be addressed in order to truly achieve an inclusive process of responsible research and innovation in digital agriculture.

In conclusion, digital agriculture presents challenges, especially for farmers. States introducing digital agriculture and related policies, should be mindful of the fact that they are bound by obligations under the human right to science. A way to comply with these obligations but also to guide digital agriculture towards a model oriented towards serving society's needs is RRI. The approach of RRI is only one example of pre-emptive policies (including for example human rights impact assessments) which would help address the risks of digital agriculture in an effective way i.e. through the anticipation of such risks and the adoption of timely legislation to address them.

7.2 Impact of New Technologies Used and Developed by the State of Israel on Human Rights

By ***Veronika D'Evereux*** (Charles University and CEVRO Institute)

Introduction

The presence of new technologies based on artificial intelligence (AI) is a reality that influences lives of individuals in various ways. It can be assumed that the use of these technologies will continue to expand, with an increasing number of people using them, and new programs, machines, or devices based on them will be developed. However, the use of these technologies has an impact on the realm of human rights protection. Some technologies might have positive impact and might be beneficial for the development and implementation of human rights, especially the rights relevant to the quality of human life. But it may also lead to their violation.

The aim of this paper is to examine the technologies developed and used in the State of Israel in the context of the laws of human rights. There were formulated two research questions. Whether and what human rights could be possibly violated by these AI systems? How should these technologies be used, so they do not interfere with the existing laws of human rights? The structure of this paper corresponds with this aim. The first chapter briefly explains the current stage of the problematics of missing universal legally binding rules for use of the artificial intelligence, which would also reflect the protection of the human rights. The second chapter summarises the AI technologies and systems operating on the basis of AI which are developed and used in Israel, and it explains in what areas these technologies can be used. The third chapter is focused on the potential positive as well as negative impact of the examined technologies on human rights. The research questions are answered in the conclusion of this paper.

1. Legal definition of artificial intelligence, the lack of universal binding rules for its use and the risk of the human rights infringement due to the use of new technologies

The protection of human rights under international law applies to individuals regardless of their nationality, both in times of peace, and during armed conflicts. This legal framework is stipulated in international customary law, with some of these human rights rules having the nature of peremptory norms (*jus cogens*). It is also present in multiple universal and regional international treaties.[824] Unlike the existing rules for the protection of human rights, universally valid legally binding rules for the use of artificial intelligence and related new technologies have not yet been established.

[824] Šturma P, Čepelka Č, *Mezinárodní právo veřejné,* 2. vydání [Public International Law, 2nd edition] (C. H. Beck, 2018), p. 260.

The first legally binding document with a regional scope titled the *"Artificial Intelligence Act"* was passed on March 13, 2024, and it should come into force in 20 days after being published in the Official Journal of the EU. It includes the definition of the AI systems, which is as follows: *"a machine-based system designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments."*[825] This act is not legally binding for the countries outside the EU. Another significant progress in terms expressing the broad interests of the states to stipulate in the future the rules for use of the AI systems and to ensure the protection of the human rights in connection with the use of the AI can be seen in the UN General Assembly Resolution A/78/L.49 which was passed on March 21, 2024.[826]

The development of new artificial intelligence technologies and their practical use is particularly relevant in the areas of national security, cybersecurity, banking and finance, transportation, education, communication, labour, and manufacturing, and, last but not least, healthcare.[827] It can be stated that AI-based technologies in their development and practical applications are far ahead compared to the emergence of related legal regulations.

Currently, discussions mainly revolve around whether the use of certain new technologies with elements of artificial intelligence should be prohibited or regulated. Given the ongoing development of these technologies, it is rather unlikely that outright bans on the use of certain technologies would be effective. Therefore, defining legal rules for their use appears to be a more realistic approach. Until the establishment of a special legally binding regulation governing the use of new technologies and artificial intelligence in connection to the protection of human rights, existing commitments of the states can and should be applied to ensure that these new technologies are not used in contrary of these commitments.

The use of AI systems touches upon a broad spectrum of fundamental human rights, mainly the right to privacy, data protection and non-discrimination. Modern technologies can pose challenges, especially concerning privacy protection,[828] and the privacy of electronic correspondence.[829] Additionally, AI systems might have impact to the right to human dignity, social security and assistance, the right to good governance (AI systems used in public administration and the public sector), consumer protection rights, the prohibition of discrimination, personality and personal data protection.[830]

---

[825] Artificial Intelligence Act, EU, P9_TA (2024)0138, 13 March 2024.

[826] UN General Assembly Resolution A/78/L.49.

[827] Antebi L, 'Artificial Intelligence and National Security in Israel.' Memorandum No. 207 (*INSS Tel Aviv University*, 2021) <https://www.inss.org.il/publication/artificial-intelligence-and-national-security-in-israel/>.

[828] which might be related to the devices responding to voice commands and thus constantly "listening," or applications allowing the automatic editing of photos to create images of nude individuals.

[829] which might be related to various apps for text and voice communication, the content of the communication might be monitored.

[830] European Union Agency for Fundamental Rights, 'Getting the Future Right. Artificial Intelligence and Fundamental Rights', Report, Luxembourg: Publication office of the European Union, 2020, p. 7.

While the automation of various systems can significantly enhance their efficiency, it is crucial to ensure that AI-based decisions are non-discriminatory. Rigorous testing to uncover potential biases in AI decision-making and subsequent verification by humans might be essential for the practical use of these systems.

When it comes to the use of AI systems in practice in a way that would have impact on human rights, this should be done while respecting the principle of proportionality and the principle of necessity. Furthermore, the principle of legal certainty should be also respected, which is essential both for the developers of these systems and for their users, which may affect, among other things, supervision in the field of banking, financial services or personal data protection, in the field of healthcare and various certification programs.[831]

Considering that these new technologies are constantly developing and are truly diverse in terms of the spectrum of areas in which they are used, it is desirable to continuously assess and evaluate the impact of these technologies on the protection of human rights.[832] In practice, however, it may happen that new technologies are assessed or researched mainly from the point of view of their technical aspects and methods of use, but the impact of these technologies on human rights is much less evaluated, or possibly this assessment might focus mainly on cases where technology would affect human rights in a negative way.

2. Technologies operating on the principle of artificial intelligence developed and/or used in Israel

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 leaders (besides the USA and China) in the AI technologies by 2030.[833] Israel has a powerful technological strength and is often referred to as the "start-up nation" because of the large number of start-up companies in comparison to the size of its population. Israel understands that it is necessary to compensate its lack of natural resources and limited human resources by investing in human resources and technologies and focusing on developing the national security strategy is the key to success. This for example reflects the fact that Israel is one of the world's largest weapons exporters and the level of the Israeli security industries turned Israel into a technological and economic power.[834] Many countries in this aspect rely on Israel. The competitive advantage of Israel's security industry is its close relationship with Israeli Defence Forces (IDF) which is interconnected with research, academia,

[831] See, Antebi L, 'Artificial Intelligence and National Security in Israel.' Memorandum No. 207 (*INSS Tel Aviv University*, 2021) <https://www.inss.org.il/publication/artificial-intelligence-and-national-security-in-israel/>.

[832] Ibid., pp. 8–9.

[833] 'Artificial Intelligence (AI) and the government data revolution' (*INDA*, 19 July 2022) <https://tinyurl.com/5n6upvsn> accessed 29 October 2023.

[834] Sheer S, 'The State of Artificial Intelligence Israel' (*Innovation Center Denmark*, 2019) <https://tinyurl.com/3ukee298> accessed 29 October 2023.

development and implementation process that operate cooperatively, share ideas and human capital.[835]

There can be noted an approach to distinction the AI technologies into two main groups, this distinction is proposed by the IDF. The first category includes the technologies which replace "hard workers", which includes the systems allowing automatic decoding, automatic translation and other extremely time-consuming tasks. The other category includes systems which help humans to make decisions and that are in some cases capable to take autonomous decisions about the tasks, and also the technologies which are capable of planning and forecasting.[836] Many technologies are influenced by the AI and sometimes other technologies are required to enable or support application of the AI. These are some of the most relevant technologies: robotics, swarms, human-machine interaction technologies, brain-machine interaction technologies, big data systems, super-computing systems, quantum computerization systems, cloud computing systems and 5G networks.

Robotic devices have existed since 1960s.[837] Current robots are able to analyse new situations, examine the environment and act accordingly, some are even able to relate to human emotions. AI is an important component of these robots as it works as their "brain" because it controls the physical part of the robots which are able to perform wife range of missions and tasks including autonomous driving, transporting goods, manufacturing products, cleaning and many other tasks in various fields. Robotic systems became increasingly autonomous, and their potential is still growing, therefore their use is connected with complex legal and ethical issues.[838] Israel already in 1960s and 1970s used unmanned aerial vehicles (UAVs) / drones for photographic purposes and for information gathering. In the Second Lebanon War in 2006 the drones played significant role. Israel is one of the main leading countries in the UAVs market as well as is one of the leading countries in developing, producing and sing other unmanned systems, some of them enjoy a level of autonomy. These systems include unmanned patrol vehicles, ground robotic systems, loitering munitions such as the Harop and the Harpy.[839] Israel is also focused on the autonomous automotive industry, on development complementary technologies for autonomous systems, such as sensors and navigation systems and Israel is also involved with testing of autonomous vehicles.[840]

When it comes to the right to life, the autonomous weapon systems (AWS), which fall into the above-mentioned category of robotic systems, obviously represent very serious risk. The AWS can be used on the battlefield and have various applications, ranging from defence systems to systems for conquering and attacking targets on land, air and sea. These systems are lacking human compassion and sensitivity. The international

---

[835] Antebi, c. d. pp. 83–85.

[836] Antebi, c. d. pp. 47–48.

[837] While the word "robot" was first used in 1920 in science fiction play R. U. R. (Rossum's Universal Robots) written by Karel Čapek; the author of the word was in fact his brother Josef Čapek who suggested using this word to describe the artificial workers.

[838] Antebi, c. d. p. 53.

[839] Ibid., p. 87.

[840] Ibid., p. 88.

law prohibits targeting civilians. Therefore, the AWS might not have the decisive ability to distinguish between civilians and combatants. In addition, when attacking a soldier, the international law requires respecting the principle of proportionality, which means the attack should be aimed at making the soldier unable to actively participate in the armed conflict (as opposed to killing the soldier). There is also unresolved the question of responsibility when it comes to use of AWS, this doubt would be answered under the current stage of law in case there was a human being responsible for the decision making, therefore by using semi-autonomous weapon systems when the human being is responsible to activate the weapon towards the target.[841] Similarly, in relation to right to life, there could emerge legal dilemmas when the robotic systems are used in medicine or in the traffic, especially when the systems endanger human life.[842]

Swarms intelligence is a field of AI which imitates animals operating in groups, mainly bees and ants. Members of swarms share a common intelligence which overlap among individuals within their group. The swarms AI systems include software and hardware capable of making its own decisions which are interconnected because of analysing the information from its all parts, therefore the system takes the best decisions for the whole group of swarms. The swarms have the ability to successfully perform the task even if some of the swarms get disabled. In that case the swarms technology restarts its activity and perform the task based on the new data. This ability brings swarms a lot of advantages compared to the AI technologies which operate individually.[843] In 2021 Israel was supposedly first country in the world, when deployed the drone swarms above Gaza.[844]

Human-Machine Interaction technologies include various subfields of the AI which enable easy and effective interaction between machines and people. These technologies are capable of spoken language analysis, they can chat, they can analyse human emotions. Among the most known technologies in this category are the personal assistants Siri and Alexa[845] or Chat GPT. Israel Innovation Authority is investing over 8 million USD to facilitate and advance the development of this area of AI in Hebrew and Arabic language.[846]

Brain-Machine Interaction technology is a comprehensive name for devices which communicate with computers through brain activity alone. These technologies are capable of translation the neurological information into commands which allows them to control software and hardware. These technologies operate as if they were able to "read the human thoughts". The practical use of these technologies is in medical application, for example the robotic limbs and cochlear implants (hearing devices) work on this

[841] Wagner M, 'The Dehumanization of International Law: Legal, Ethical and Political Implications of Autonomous Weapon Systems' (2014) 47 *Vanderbilt Journal of Transnational Law* 1371, pp. 1399-1405.

[842] Antebi, c. d. p. 78.

[843] Peters J, 'Watch DARPA Test Out a Swarm of Drones' (*The Verge*, 2019) <https://tinyurl.com/bmjr52t9> accessed 21 October 2023.

[844] 'In apparent world first, IDF deployed drone swarms in Gaza fighting' (*The Times of Israel*, 2021) <https://tinyurl.com/uj6yuvfe> accessed 30 October 2023.

[845] Getz D et al, *Artificial Intelligence, Data Science, and Smart Robotics: First Report* (Haifa, 2018), p. 63.

[846] Israel allocates NIS 30M to fund projects for AI applications in Hebrew and Arabic. In: The Times of Israel, 2023 <https://tinyurl.com/3spdwf3x> accessed 30 October 2023.

base.[847] These technologies also have potential in the field of security, these systems can improve the cognitive abilities of soldiers through the brain-machine interaction.[848] Currently, there are ongoing studies, for example at Bar Ilan University in Israel focused on the bridges between neurosciences and machine learning.[849]

Big Data systems are enormous amounts of data, sometimes compared to large and complex databases, the management of these systems and manipulation with them involves logistic challenges and therefore it cannot be done by using usual data processing methods and applications. The Big Data systems are used to train AI due to the fact that significant and valuable patterns can be learned from its analysis.[850] There are more than hundred companies in Israel which are focused on developing this area of AI.[851]

Super-Computing systems refer to computers that have powerful calculation capabilities, they are designed to solve a single problem by a specific calculation. Super-computers are for example used to develop nuclear weapons.[852] In 2021 Israel allocated around 8 million USD to finance the Israel's official national supercomputer project.[853]

Quantum Computerization systems are based on quantum mechanics, they operate on the basis of quantum superposition and entanglement, and they generate high-level computing abilities. While "normal" computers perform calculations using binary units, quantum computers use qubits (they can be both 0 and 1 at the same time). These systems can create new paradigms in the way how they collect, store and process information, they can be used in security areas, because they have the ability to disrupt all the usual methods of encryption and therefore cause the collapse of the existing systems.[854] In the last approximately 5 years there has been established at least 30 quantum computing companies, Israel allocated 29 million USD to establish Israeli Quantum Computing Centre (currently in progress).[855]

Cloud Computing systems allow the access from any location to the shared pool of resources including networks, servers, storages, applications, services and data. These systems allow remote computer which is connected to the network to access the database. The Cloud Computing systems have the ability to use the resources, platforms and software through the provider's websites. Cloud computing can store large amounts

---

[847] Gonfalonieri A, 'A Beginner's Guide to Brain-Computer Interface and Convolutional Neural Networks' (*Medium,* 2018) <https://tinyurl.com/ycxrys6x> accessed 21 October 2023.

[848] Marsh S, 'Neurotechnology, Elon Musk and the Goal of Human Enhancement' (*The Guardian*, 2018) <https://tinyurl.com/nhcnekrh> accessed 21 October 2023.

[849] 'Israeli scientists study secrets of human brain to bring AI to next level' (*The Jerusalem Post*, 2020) <https://tinyurl.com/yr2vmkc8> accessed 21 October 2023.

[850] Press G, '12 Big Data Definitions: What's Yours?' (*Forbes*, 2014) <https://tinyurl.com/uf22kvr5> accessed 21 October 2023.

[851] '101 Best Israel Big Data Startups & Companies' (*Data Magazine*) <https://tinyurl.com/bddvzz8z> accessed 21 October 2023.

[852] Antebi, c. d. pp. 55–56.

[853] 'Israel wants a massive supercomputer – no matter the costs' (*Haaretz*, 2021) <https://tinyurl.com/3879rp9f> accessed 21 October 2023.

[854] Ibid.

[855] 'Is Israel about to become a leader in quantum computing?' (*Israel21c*, 2022) <https://tinyurl.com/2a5scm6k> accessed 31 October 2023.

of data and the AI systems can access it to get training or to make decisions. The AI can also enter new data to cloud.[856] Cloud Computing is another area of Israel's interest in research and development, there seem to be currently about 5 leading companies in Cloud Computing.[857]

5G networks enable and improve the performance of AI systems by allowing transferring huge amounts of data while the AI can reciprocate by understanding the complexity of 5G networks and the information these networks produce.[858] In 2023 he State of Israel allocated over 6 million USD for a program to conduct research in various public sectors through the 5G technologies, this project is also supposed to promote Israeli hi-tech industry, mainly the companies which focus on communication solutions for communication operators around the world.[859]

This chapter can be concluded by some additional considerations. Despite the ongoing development of the AI systems, there are still a lot of challenges stemming from the use of the AI and the technologies operating on its basis. First, there is no international standard for the safety of AI, therefore the AI could have various defects when entering the market. For example, the technologies could be discriminative towards certain groups of population. The AI could become a safety risk, the technologies could become highly independent and therefore get out of human control. Therefore, when it comes to the area of fully autonomous weapon systems, it might be relevant to consider, whether the use of the fully autonomous weapon systems should be completely banned by a treaty with similar effects like the Convention on Certain Conventional Weapons.[860] Second, the AI might have a negative impact on the areas of armament, including nuclear armament. Some scientists speak of a "hyper war" which is a war carried out with use of AI allowing automated decision making without the possibility of having the human decision-making process present.[861] Third, the use of AI might widen the gap between well-developed and developing countries which might become even more limited in operating at the international arena. This gap might be one of the reasons for large migration waves. Groups of inhabitants in developing countries might also use violent measures, for example terrorism, because of their inability to cope with this growing gap.[862] In contrary, the AI can have a great benefit, for example it can strengthen the countries with small or aging population. It can positively increase the global economic growth rate. The AI can help to find cure for illnesses and improve

---

856 'What Is Cloud Computing?' (*Amazon*, 2020) <https://tinyurl.com/2jp2s4bm> accessed 21 October 2023.

857 'Israel is in the front line of cloud computing era' (*Economic and Commercial Mission Consulate General of Israel in Hong Kong*, 2022) <https://tinyurl.com/mryufbw8> accessed 31 October 2023.

858 Yost S, 'Brave New World: Everything Gets Smarter When 5G and AI Combine' (*Electronic Design*, 2019) <https://tinyurl.com/ppatnfp4> accessed 21 October 2023.

859 'Israel IT government encourages 5G cellular Innovation' (*ITA*, 2023) <https://tinyurl.com/6s42fec2> accessed 31 October 2023.

860 Antebi, c. d. p. 73.

861 Allen JR and Hussain A, 'On Hyper War' (*Fortuna's Corner,* 2018) <https://tinyurl.com/3me68xke> accessed 21 October 2023.

862 Zimmermann E, 'Globalization and terrorism' (2011) 27 *European Journal of Political Economy* 1.

health systems. It can improve the efficiency and safety of transportation; and finally, it can encourage energy efficiency and improve the understanding of climatic changes.[863]

3. Some insights on the impact of the new technologies on protection of human rights and the human rights protection in the perspective of Israeli National Security concept

The final chapter is aimed at pointing out some areas of possible impact of the new technologies operating on the basis of AI on human rights.

The Israeli National Security Doctrine (INSD) is a concept focusing on protection Israeli citizens (and their human rights) and the state from its internal and external security threats, including hostile states and terrorist organisations. Nevertheless, this Israeli National Security concept is not completely unique. As a comparison there can be noted for example UN concept of national security which includes economic safety, food safety (preventing famine and lack of food), health safety (preventing diseases, avoiding food contamination, malnutrition and lack of access to basic medical care), environmental safety (preventing environmental damage, depletion of resources, natural disasters and pollution), personal security (preventing physical violence, crime, terrorism, domestic violence, child slavery), community security (applying measures against ethnic, religious and identity based tensions), and political security (taking measures against political repression and human rights violation).[864]

The Israeli National Security Doctrine was accepted by a government committee led by Dan Meridor in 2006 and later on adopted by the minister pf defence Shaul Mofaz.[865] The INSD has 4 main areas which are: "*Ensuring the survival of the State of Israel and protecting its territorial integrity and the security of its citizens and inhabitants*; *Protecting the values and national character of the State of Israel, as a Jewish and democratic state and as the home of the Jewish people; Ensuring the State of Israel's ability to maintain its socioeconomic strength, like any other advanced country; Reinforcing the State of Israel's international and regional standing and seeking peace with its neighbours.*"[866]

This program might be relevant to the issue of the human rights protection and the use of the new technologies based on artificial intelligence in several aspects. It, for example, explains why the cyber security became the key factor of the highest degree in the military concept of deterrence, defence, and attack. The IDF strategy includes four basic aspects which are relevant to all military actions, these aspects are attacking, defensive, assisting and enabling. Therefore, having technological superiority with AI is crucial for the State of Israel. AI has been used in aerial defence systems.

[863] Antebi, c. d. p. 75.

[864] Human Security in Theory and Practice, United Nations Office for the Coordination of Humanitarian Affairs, 2009 <https://tinyurl.com/2p8fscuy> accessed 21 October 2023.

[865] Just as an interesting note, it can be mentioned that this concept was never approved by the entire Israeli government.
Meridor D and Eladi R, 'Israel's National Security Doctrine: The Report of the Committee on the Formulation of the National Security Doctrine (Meridor Committee). Ten years later.' (*INSS*, 2019) <https://tinyurl.com/ysteeveh> accessed 21 October 2023.

[866] Ibid., see also, Sheer S. c. d. pp. 17–18.

IDF uses AI in military intelligence and telecommunication which helps to improve the warning systems. AI is also used in operational learning and planning; the AI can reach conclusions which were impossible to reach in the past with human efforts due to difficulties in handling and analysing vast amount of data.[867]

Aside of the aspect of artificial intelligence, there could be noted several aspects which might be found problematic in connection to the general concept of protection of human rights. One of them would be avoiding mentioning the minorities living in the State of Israel. This omission in the above cited text might raise questions whether such approach is really democratic. Including the aspect of the artificial intelligence, there could be raised concern whether these technologies might be operating fully in accordance with the ***prohibition of discrimination*** which might contain multiple aspects not only in relation to the wide content of this human right, but also in relation to the broad variety of the technologies. There can be given several examples to create some general idea of the problematics.

These technologies can be used in a different way in connection to Jews and Arabs. Antebi noted that "*the AI system is only as good as the data it accepts. When the data used to train the machine is not sufficiently diverse, biases may arise.*"[868] But even when "the data is perfect", it still reflects social bias, such as gender and ethnic differences. This is potentially very dangerous in using military AWS. This is exceptionally relevant for the IDF given the fact that the Palestinian terrorists are often women, and not exceptionally children (persons under the age of 18). The terrorists very often purposely do not use any outer sign which would allow them to be distinguished from civilians. On the top of that, the terrorists from Hamas and Palestinian Islamic Jihad also often dress up as Jewish people, sometimes they even wear Israeli police uniforms.[869] The fully autonomous AI weapon systems might face challenge of distinguishing between the civilians and combatants, which is another problem because 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 a little 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. One of the options of how to eliminate the risk of violation of the international law of armed conflicts might be stipulating, that the developers of the AI should consult their inventions and results of testing with lawyers who are specialised on this area of law, which, after all, could be suggested in regards many other types of weapons.[870]

---

867 'Israel Defence Force Strategy Document' (*Harvard Kennedy School Belfer Centre for Science and International Affairs*, 2015) <https://tinyurl.com/j3d63npb> accessed 21 October 2023.

868 Antebi, c. d. p. 105.

869 Lately in the 7 October 2023 terrorist attack.
'The terrorists wore our uniforms. IDF soldiers recount the liberation of Israeli communities' (*i24News*, 2023) <https://tinyurl.com/4u72esn8> accessed 21 October 2023.

870 Of course, there is a likelihood that the developers might object such a rule or condition. The consultations with legal experts and possibly also the manufacturer's obligation of implementation the legal recommendation or findings into the AI programs might either significantly slow down the development, or it might even prevent some technologies from being completed. This could lead into a financial loss, so the investors in the AI technologies might object that too.

There are currently several AI software technologies which are capable to create a realistic looking photograph or to edit the existing photograph in a way that it significantly changes its content. This might be potentially a big risk of the AI technologies in connection to the prohibition of discrimination because when these technologies are misused, for example in order to support war propaganda, they might have enormous impact on influencing public opinion.[871] There stems another problem from the technological possibilities of these technologies. That is a misuse of the AI systems for the purpose of creating fake news which have significant impact on forming and influencing public opinion. It might be benefiting, if there is launched some information campaigns which would offer easily understandable information to the public. The people should be able to learn about the most important aspects of use the AI in order for them being able to distinguish the most important areas related to the AI, and its impact to human rights protection. Or perhaps there could be at least included some sort of mandatory note informing the readers that the content is not verified, and that the information might be misleading.[872]

There might be also a concern regarding ***right to privacy*** including privacy of communication when it comes to the military AI telecommunication technologies which are used to improve warning systems. 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, in the civilian objects including the civilians who live in the refugee camps is one of the common and generally known problems.[873]

The spyware might interfere with the right to private life and from the perspective of the international law, therefore it should be always well evaluated, how proportional is it in the context of the security threads Israel deals with. On one hand, it might be reasonable for the IDF to use these technologies as it might appear proportional considering the huge security threads, armed and terrorist attacks that Israel has been facing ever since. On the other hand, since it is not an option for the people using the technologies to choose whether their communication can or cannot be monitored for the security purposes, there should be at least provided a clear as well as brief information to the users, so they are aware of the terms and conditions of the services they use.

Another concern of AI might be in connection to ***right to work***, in other words to the job market and employment. Such a concern is not completely new, similar concern was raised during the industrial revolution in 18th and 19th century. The development of the AI could create new jobs for people, improve the efficiency in industry and services,

[871] 'AI has made the Israel Hamas misinformation epidemic much, much worse' (*Rolling Stone*, 2023) <https://tinyurl.com/2kpprcay> accessed 1 November 2023; 'Pro-Hamas narratives on social media getting pushed by fake accounts firm says' (*Fox Business*, 2023) <https://tinyurl.com/4ppe28pt> accessed 01 November 2023; 'Social media platforms swamped with fake news on Israeli Hamas war' (*Al Jazeera*, 2023) <https://tinyurl.com/5xbpdxvt> accessed 1 November 2023.

[872] 'How we address misinformation on X' (*X Help Centre*) <https://tinyurl.com/37ec2pav> accessed 25 November 2023.

[873] 'The Gaza Metro: The mysterious subterranean tunnel network used by Hamas' (*CNN*, 2023) <https://tinyurl.com/ycyv5usd> accessed 21 October 2023.

increase supply and lower prices. That could lead to growth in private consumption and that will encourage the expansion of the global economy.[874] At the same time it could cause that some professions might disappear from the job market, which might be currently relevant to the workers in the fields of knowledge and information, who might be replaced by AI. The employees, in order to succeed in the labour market, might need to become more flexible and there might emerge a need to develop new skills and ability to adapt to the changing reality. This might be a challenge for developed countries, including Israel, because they might become required to change their approach to education and employment and to create systems which will enable lifelong learning and development. The state support system and the laws of employment might also need to adapt to the new reality in order they are able to support various population sectors and their needs.[875] It is possible to debate whether in several years the AI software will be able to perform better work than people. For example, in connection to writing and translating text, this might not be that far away in the future as far as of for example the Chat GPT software.

These technologies might therefore have both, pros, and cons in connection to right to work. On one hand it could cause a crisis in the area of human occupation. There could be created completely new professions and forms for work, these technologies have a great benefit for those who prefer to work remotely. But on the other hand, these technologies might have a negative impact to the right to work of those who perform manual work and who are unable or not interested to change their career. These technologies might have, in the future, the capability to replace some manual workers. Still, it is probably unlikely that these technologies would in the near future eliminate or endanger a significant percentage of manual workers.

The technologies might also have a great impact on the ***right to an adequate standard*** of living, on the ***right for the continuous improvement of living conditions*** and on the ***right to achieve the highest attainable level of physical and mental health***. The robotic technologies which are currently being developed and which operate based on artificial intelligence and brain-machine interaction might significantly improve the quality of life of disabled persons, persons who suffered injuries. These technologies could help these people to be much more independent not only in the area of personal care and hygiene, but in general, these technologies could help the disabled people to enjoy similar quality of life comparable to healthy persons, so the people might not have to rely on the assistance of care takers.

As stated above, it is rather unrealistic that these technologies would massively substitute the human work in the near future. And even if this might happen in the more distant future, there might still be need for the presence of the human care takes as the recipients of the social services might prefer to continue having the possibility of interaction and communication with the human beings, so the care takers could provide the emotional comfort and companion, while the machines could do the "hard work".

---

[874] Hawksworth J, 'AI and Robots Could Create Many Jobs as They Displace' (*World Economic Forum*, 2018) <https://tinyurl.com/2kd5cjn3> accessed 21 October 2023.

[875] Antebi, c. d. pp. 110–111.

As much as the intentions of the developers might be good and the AI technologies should be only benefitting to mankind, there might be a risk of unauthorised change of programming of the software operating for example the artificial limbs or software which communicates with human brain. Therefore, there should be some sort of legal rule, that these AI technologies must have a security measure, which in case the software gets hacked, the artificial limb or medical device (for example a wheelchair or a lift operating based on AI) will immediately stop operating and the human service operator will be automatically called to check the device and fix the problem. It might be also discussed, whether there should be accepted a legally binding rule, that the artificial intelligence must not change the physical nature of a human being. In the author's opinion, there might be strong ethical grounds for such prohibition.

Conclusion

In order to fulfil the aim of this paper, there are answered the two research questions.

In connection with the first research question focused on examining on whether and what the human rights could be possibly violated by the AI systems, following can be stated. In the chapter three, there were mentioned the major areas of human rights, with which the AI systems might interfere with. Those were prohibition of discrimination, right to privacy and right to work. This includes the systems that are used in military, security as well as civil context. The potential risk of human rights violation is mainly due to the technological aspects of these systems and the options as well as outcomes which stem from their use. The author also noted in the chapter three several areas of human rights to which the AI systems might have benefit impacts due to the technological possibilities of these systems. Those are the right to an adequate standard of living, the right for the continuous improvement of living conditions and the right to achieve the highest attainable level of physical and mental health. The more these technologies are expanded and used in various areas, by public authorities for civil, security and military purposes, as well as by private individuals, the greater will be the need to ensure that a large-scale and serious violation of human rights is prevented from happening. This might occur due to deficiencies in the functioning of these technologies, especially if the decisions taken by the systems are not verified by responsible human operators.

In connection with the second research question focused on examining on how these technologies should be used, so they do not interfere with the existing laws of human rights, following can be stated. The AI systems should always remain under human control mainly due to the prevention of creating situations which are not regulated by any currently valid laws. The existing legal rules stipulating the issues of accountability, responsibility and liability are not applicable to any technologies operating on the basis of the AI. There should be clearly stipulated the rules of responsibility for the human rights violation by using AI, even if the AI systems were not directly ordered by a responsible human commander or operator. There should also be established universal legal framework for the human rights protection in relation to the use of the AI. Among other things, there should be performed regular legal assessment of impact of AI to human rights. This legal framework should also include a control mechanism. One of the options for the control mechanism might be creating an organisation which will

perform independent oversight, it will include administrative, judicial or quasi-judicial and legislative oversight. Main purpose of this control mechanism should be prevention of discrimination.

As a final remark it can be stated that the AI systems should not only be used in accordance with currently valid legal framework, but they should neither be used in the way which is contradicting to the subject and purpose of the existing legal protection.

7.3 Border Deaths on the Rise? Navigating Risk through Technologies of Control

By ***Aphrodite Papachristodoulou*** (University of Galway)

Introduction

On 14 June 2023, the second deadliest shipwreck on record in the Mediterranean Sea since 2015 occurred in the open waters of Greece, near the tourist island of Pylos. Approximately 750 individuals were traveling on the boat of whom 104 survived the wreck, 78 were recorded dead and the remaining, approximately 600, missing and presumed dead. As unpalatable as this may seem, this is a case where migrants called for help, several actors witnessed and came in close proximity with the boat in distress and yet all the parties involved *chose* to remain inactive. Since this boat sinking, the death toll has not stopped; rather, it has steadily increased. The calls for accountability and an end to the practice of abandonment at sea, which undermines well-established obligations of international law are countless. Relatedly, the risk of death associated with migration by sea is especially high due to drowning, malnourishment, suffocation, dehydration, starvation, unsanitary conditions and violence.[876] Hence, the thousands of lives that perish each year in the Mediterranean region have become a humanitarian concern that is growing in scale and demanding significant attention.

Under the international law of the sea framework, the principle of saving lives of those in distress at sea becomes of critical importance for safeguarding the right to life under international human rights law, as both share the same purpose: the protection of human life. Apart from being a long-standing and fundamental tradition of seafaring, this humanitarian norm is also incorporated as a legal duty of the search and rescue (SAR) system under international law.[877] In the last decades the attention of saving lives at sea and preventing deaths that occur once people embark on perilous sea journeys has diverted towards the protection of borders.[878] Accordingly, the European Union (EU) and its Member States have drawn migration control policies,[879] concluded bilateral cooperation agreements with third countries,[880] and fortified external borders,

[876] Ghráinne M, 'Left to Die at Sea: State Responsibility for the May 2015 Thai, Indonesian and Malaysian Pushback Operations' (2017) 10 *Irish Yearbook of International Law*, p. 7.

[877] United Nations Convention on the Law of the Sea (adopted 10 December 1982, entered into force 16 November 1994) 1833 UNTS 397 (UNCLOS), Art. 98.

[878] Spijkerboer T, 'Moving Migrants, States, and Rights: Human Rights and Border Deaths' (2013) 7(2) *Law and Ethics of Human Rights* 213, p. 213.

[879] E.g., Council of the European Union, Council Decision (CFSP) 2013/233/ of 22 May 2013 on the European Union Integrated Border Management Assistance Mission in Libya (EUBAM Libya) [2013] OJ L138/15.

[880] E.g., 'Memorandum of understanding on cooperation in the fields of development, the fight against illegal immigration, human trafficking and fuel smuggling and on reinforcing the security of borders between the State of Libya and the Italian Republic' (*EU Migration Law Blog*, 2017) <https://eumigrationlawblog.eu/wpcontent/uploads/2017/10/MEMORANDUM_translation_finalversion.doc.pdf>; Council of the European Union, Council Decision (CFSP) 2020/472 of 31 March 2020 on a European Union

in a manner that shift the focus of humanitarian efforts towards preventing migration flows at *all costs* – even one's life.

Against this backdrop, this contribution explores how the employment of technology (e.g., aerial and maritime surveillance drones) in the EU's external border management is transforming the way States acquire control over seaborne migrants and deconstructing traditional conceptions of border and territory. The belief that border externalization and surveillance technologies can assist in tackling migration movements is gaining momentum. Thence, the incorporation of state-of-the-art technologies has led to a sharp expansion of States' powers that has arguably become a double-edged sword. Whilst the increasingly technological nature of borders helps the EU's effort to halt irregular migration flows,[881] it also segregates mobility and has created a bulwark to accessing international protection. Relatedly, the border becomes a vital point of surveillance, where mobilities and identities are under the *remote* control of State authorities.[882] This has allowed for a risk-based approach to border management whereby technologies used and deployed do not have as their primary goal the management of migration but rather 'to remove obstacles to the function of the internal market or to fight terrorism or other forms of organized cross-border crime'.[883]

This Chapter is structured as follows. The first section presents the gradual digitalization of the border by examining extraterritorial State practices together with the evolving European policy approach in the Mediterranean region. Following, the second section documents the discernible impact of technologies on the human rights of migrants, which has resulted in border violence, the preclusion of entry and a rise in border deaths. The third section maps these practices by analysing two contemporary distress incidents that have taken place in the Mediterranean waters, documenting how State power through technologies of control has been exerted over migrants at sea from afar.

1. Contemporary Manifestations of State Power in External Border Management

By definition, migration is a source of human mobility that is best described as a geographical phenomenon characterised by the movement of people across borders and geographical spaces.[884] In Europe, third-country nationals who do not carry the requisite visa documents for legal entry are often forced to take dangerous migration journeys, with the sea route being the most prominent. Conversely, migration policies

---

Military Operation in the Mediterranean (EUNAVFOR MED IRINI) <https://eur-lex.europa.eu/eli/dec/2020/472/oj>.

881 Dijstelbloem H, Meijer A and Besters M, 'The Migration Machine' in Dijstelbloem H, Meijer A (eds), *Migration and the New Technological Borders of Europe* (Palgrave Macmillan, 2011), p. 3.

882 Amoore M, Marmura S and Salter M, 'Editorial: Smart Borders and Mobilities: Spaces, Zones, Enclosures' (2022) 5(2) *Surveillance & Society* 96, p. 97.

883 Rijpma J, 'Brave New Borders: The EU's Use of New Technologies for the Management of Migration and Asylum' in Cremona (ed), *New Technologies and EU Law* (OUP, 2017), p. 209.

884 Könönen J, 'Legal geographies of irregular migration: An outlook on immigration detention' (2020) 26(5) *Population Space and Place* 2340, p. 5.

to control or set entry requirements in a country or group of countries, like the EU, have a geographical dimension.

While States and the international community have not remained idle to the thousands of migrants that perish each year, their response has been rather tailored to averting the 'threat' posed by irregular migration to their territoriality sovereignty.[885] In addressing this phenomenon, contemporary manifestations of State power have been increasingly witnessed through the use and deployment of technology in external border management. Such technological border control practices are best characterized by the risk logic which primarily deals with the anticipation and active prevention of undesirable events rather than with the existence of existential threats.[886] By way of illustration, precaution oriented strategies of border surveillance including aerial and maritime drones have been utilized as pre-frontier detection and monitoring mechanisms, enhancing in this way a State's *capacity* to control migrant boats. Advanced technologies such as sea-bed and ground sensors, satellite and aerial video surveillance, thermal imaging cameras, Unmanned Aerial Vehicles (UAVs), and even experimental robotic technology are deployed to monitor and control movement before individuals reach a country's physical borders.[887]

European States have enormously invested and employed technologies of control and surveillance that have as the primary goal to tame migration in the Mediterranean, thereby treating the sea as a border to halt migration flows at *all* costs.[888] In this way, technologies are not merely the result of a risk-based approach to migration, but they also enable it serving both as a factor and an outcome of treating cross-border mobility as a security concern.[889] This can be particularly traced first by the establishment of the European Border Surveillance System (EUROSUR) in 2013, a program that is operated by the EU's Border and Coast Guard Agency (Frontex) that uses big data technologies (including satellite imagery and ship recording services) 'to predict, control and monitor

---

[885] Papastavridis E, 'Rescuing Migrants at Sea and the Law of International Responsibility' in Gammeltoft-Hansen T and Vedsted-Hansen J (eds), *Human Rights and the Dark Side of Globalisation: Transnational Law Enforcement and Migration Control* (T&F, 2016), p. 161.

[886] Niemann A and Schmidthäussler N, 'The Logic of EU Policy-Making on (Irregular) Migration: Securitisation or Risk' (*Mainz Papers on International and European Politics*, 2012) <https://international.politics.uni-mainz.de/files/2014/07/mpiep06.pdf>, p. 13.

[887] Kapogianni V, 'The Reverberations of the Rise of Fencing Border Regimes: Pushbacks, Detention and Surveillance Technologies' (*International Law Blog*, 21 November 2022) <https://internationallaw.blog/2022/11/21/the-reverberations-of-the-rise-of-fencing-border-regimes-pushbacks-detention-and-surveillance-technologies/>. Also, other AI technologies deployed at external borders include integrated analysis of various data streams including Automatic Identification Systems (AIS), coastal and vessel-mounted sensors, and contextual information concerning the weather, commercial activities, environmental conditions, military exercises and maritime incidents, see also European Border and Coast Guard Agency, 'Artificial Intelligence-Based Capabilities for the European Border and Coast Guard Final Report' (*Frontex*, 2021) <https://frontex.europa.eu/assets/Publications/Research/Frontex_AI_Research_Study_2020_final_report.pdf>.

[888] Foucault M, *Discipline and Punish: The Birth of the Prison* (Vintage Books, 1975), p. 318.

[889] Rijpma J, 'Brave New Borders: The EU's Use of New Technologies for the Management of Migration and Asylum' in Cremona (ed), *New Technologies and EU Law* (OUP, 2017), p. 210.

traffic across the EU borders' and ultimately to block migrants' passage.[890] In particular, one of the aims of EUROSUR is to 'contribute to ensuring the protection and saving the lives of migrants'.[891] Despite a significant decline in the number of migrant crossings since 2016, attributed to the EU's emphasis on securitization, a disconcerting trend has resulted. This decrease has been accompanied by a notable increase in the mortality rates in the Mediterranean, as will be demonstrated below.[892] This has to be attributed, at least in part, to the failure of the EU policy and operational strategies aimed at countering the flow of migrants reaching European shores. Ergo, whilst EUROSUR could have been utilised to save migrants in distress, in practice, it primarily presents a tool to the EU to fight 'illegal immigration', adding to the proactive element of risk management. Notwithstanding where knowledge of a maritime distress situation is afforded to States through, for example, surveillance technologies producing thermal images indicating an emergency situation, this will suffice to trigger the international law of the sea obligation to render assistance without delay to those in danger of being lost at sea.[893]

In recent years, a significant deployment of aerial assets in maritime surveillance operations have come to play a key role in strengthening the EU's Mediterranean borders. This can be observed, for instance, through bilateral cooperation agreements between countries (e.g., Italy-Libya Memorandum of Understanding)[894] and joint naval operations usually conducted by Frontex. As an illustration, some of the operations in place in the Mediterranean Sea region include Frontex's Operation Themis, which has as its primary mandate border control and surveillance in the Central Mediterranean, Frontex's Operation Indalo in the Western Mediterranean, and Frontex's Joint Operation Poseidon in the Eastern Mediterranean. Moreover, Frontex has also extended its border enforcement practices to spaceborne satellites for monitoring migration flows across the Mediterranean, and in particular, has cooperated with the EU's Earth Observation Programme Copernicus, which provides satellite-based data, with the aim of enhancing the EU's external borders.[895]

Against this backdrop, technologies play an instrumental role in border management as they afford State authorities significant *power* to remotely control the passage and entry of irregular migrants.[896] Consequently, the spread of remote control signifies how

---

[890] Regulation (EU) 1052/2013 of the European Parliament and of the Council of 22 October 2013 establishing the European Border Surveillance System (EUROSUR) L 295/11, 6 November 2013.

[891] Art. 1 of the EUROSUR.

[892] See for example UNHCR, 'UNHCR data visualisation on Mediterranean crossings charts rising death toll and tragedy at sea' (2022) <https://www.unhcr.org/news/briefing-notes/mediterranean-sea-arrivals-decline-and-death-rates-rise-unhcr-calls>.

[893] Art. 98 of UNCLOS.

[894] See 'Memorandum of understanding on cooperation in the fields of development, the fight against illegal immigration, human trafficking and fuel smuggling and on reinforcing the security of borders between the State of Libya and the Italian Republic' (2017) <https://eumigrationlawblog.eu/wp-content/uploads/2017/10/MEMORANDUM_translation_finalversion.doc.pdf>.

[895] Lutterbeck D, 'Airpower and Migration Control' (2023) 28(5) *Geopolitics* 2016, p. 2022.

[896] On exclusion see, D Bigo's 'banopticon' apparatus, for instance, Bigo D, 'Detention of Foreigners, States of Exception, and the Social Practices of Control of the Banopticon' in Rajaram and Grundy-Warr (eds), *Borderscapes Hidden Geographies and Politics at Territory's Edge* (1st edn, Univ of Minnesota Press, 2007), p. 23; Tomsky T, 'Citizens of Nowhere: Cosmopolitanisation and Cultures of Securitisation in Dionne Brand's Inventory' (2019) 40(5) *Journal of Intercultural Studies* 564, p. 564.

'messy' the exercise of State sovereignty has become.[897] Evidently, sea crossings are placed under substantial (if not complete) surveillance *vis-à-vis* generating visual, ongoing knowledge by their ability to detect and trace migration movements. One might reasonably anticipate that the enhanced situational awareness would operationalize the effectiveness of SAR responses in the Mediterranean by European governments, thereby preventing further loss of life at sea by providing early warnings of distress situations as well as continuous alertness of an ongoing risk endangering life at sea.[898] Quite the opposite in fact, as this contribution goes on to show. At this juncture, it is essential to underscore that not only European border control agencies have utilised technologies, but humanitarian non-governmental organizations (NGOs) engaged in pro-active SAR in the Mediterranean have also embraced such advancements.[899] These private actors have been increasingly involved in ensuring that States are alerted about possible distress incidents and have used aerial surveillance as a tool of visibility for raising awareness among the wider public of violations of migrants' rights at sea.[900]

Underscoring the EU's strategic focus on containing migration is the fact that the EU allocates more than one and a half billion euros on research and development for security control every year, with border security and mobility management as a top priority.[901] Moreso, between 2021 to 2027, the EU has earmarked 9.3 billion Euros for border surveillance funding through the establishment of the Integrated Border Management Fund, primarily dedicated to enhancing border protection.[902] This serves as a notable illustration of the chief focus of EU policies, prompting additional questions about the significant funds allocated for surveillance and defence, which remain largely unquestioned. Such high-tech missions have the aim to spot and stop migrant vessels even before they reach Europe's borders, thereby facilitating political imperatives which carry foreseeable risks for the human rights of migrants who are stopped from accessing protection.

It follows that the EU's air surveillance relies heavily on the private sector, an opaque and unregulated web of arms lacking transparency, as well as tech companies contracted by Frontex, raising various ethical questions around the use of technologies, including AI, at borders.[903] These practices raise bewildering questions around the responsibility

---

[897] FitzGerald D, 'Remote control of migration: theorizing territoriality, shared coercion, and deterrence' (2020) 46(1) *Journal of Ethnic and Migration Studies* 4, p. 8.

[898] The vacuum of human rights protection has been specifically referred to in the jurisprudence of the ECtHR see for instance: ECtHR *Cyprus v Turkey, App no 25781/94 Judgment (10 May 2001)*, para 78; ECtHR, *Banković v Belgium, App no 52207/99 (12 December 2001)*, para 80.

[899] See, Alarm Phone, 'About' <https://alarmphone.org/en/about/>.

[900] Lutterbeck D, 'Airpower and Migration Control' (2023) 28(5) *Geopolitics* 2016, p. 2025.

[901] Binder C, 'How the EU politicises research and development in border security' (*King's College London*, 21 June 2022) <https://www.kcl.ac.uk/how-the-eu-politicises-research-and-development-in-border-security>.

[902] Nowak J, 'Drone Surveillance Operations in the Mediterranean: The Central Role of the Portuguese Economy and State in EU Border Control' (*Border Criminologies*, 26 February 2019) <https://blogs.law.ox.ac.uk/research-subject-groups/centre-criminology/centreborder-criminologies/blog/2019/02/drone>.

[903] For analysis on one's choice of AI-based technologies use, see Tasioulas J, 'The role of the arts and humanities in thinking about artificial intelligence (AI)' (*Ada Lovelace Institute*, 14 June 2021) <https://www.adalovelaceinstitute.org/blog/role-arts-humanities-thinking-artificial-intelligence-ai/>.

of the Union and its MS for human rights violations. Relatedly, in 2021, a joint report by Human Rights Watch and Border Forensics argues that Frontex and the EU's use of military drones in the Mediterranean Sea is increasingly posing a 'threat to migrants and refugees' and that 'Frontex's rhetoric around saving lives remains tragically empty as long as the border agency doesn't use the technology and information at its disposal to ensure that people are rescued promptly and can disembark at safe ports'.[904]

2. Border Deaths on the Rise

The International Organization for Migration (IOM) has recorded more than 3,105 missing migrants in the Mediterranean region in 2023 compared to 2,411 in 2022. This translates to an 11% increase in border deaths in 2023 and similarly, in 2022, there was an 18% increase from 2021. In particular, the number of border deaths started to pick up again after the pandemic year of 2020. In this light, the IOM's Global Migration Data Analysis Centre posited that the decrease in recorded migrant deaths in 2020 (1,449), does not necessarily imply that the number of lives lost truly decreased, but rather it is assumed that Covid-19 has adversely impacted the availability of data on deaths during migration by sea and the ability to track specific migration routes.[905] In this regard, from 2015 to 2018, the mortality rates in the Mediterranean region have been continuously increasingly even though the number of arrivals dropped dramatically. The stark contrast seems almost paradoxical, as one might legitimately expect to see that the fewer people making such crossings would result in fewer fatalities. While 2015 is the year when the 'European migration crisis' was formally announced, only 4 deaths per 1,000 crossings were recorded in contrast to 20 deaths per 1,000 crossings in 2018. The figures represent a fivefold increase in the death toll just three years after significant policy shifts aimed at tackling the crisis.

Even more alarming are the deaths/missing migrants recorded in the Central Mediterranean route (between Italy, Malta and Libya), which is also the most heavily surveilled area and the deadliest migration route in the world to date. One would have legitimately expected that the fact that there is such an enhanced situational awareness in that specific sea route would have contributed to fewer deaths. On the opposite, the year of 2023 so far has seen 2,476 deaths, when compared to 1,553 for the whole of 2022 and 1,000 for the whole of 2021 which make the majority of deaths in the whole Mediterranean region.

For instance, the use of surveillance technologies along the US-Mexico (land) border has revealed a twofold increase in migrant deaths and redirected crossings towards more perilous routes, particularly through the Arizona desert.[906] Similarly, it is anticipated that Europe would likely witness a similar rise in 'watery graves',[907] because of its increasing use of surveillance technology aimed at facilitating the interception and push-backs

[904] Human Rights Watch, 'EU: Frontex Complicit in Abuse in Libya' (*Human Rights Watch*, 12 December 2022) <https://www.hrw.org/news/2022/12/12/eu-frontex-complicit-abuse-libya>.

[905] Ibid.

[906] Molnar E, 'Territorial and Digital Borders and Migrant Vulnerability under a Pandemic Crisis' in Anna Triandafyllidou (ed.), *Migration and Pandemics* (IMISCOE Research Series, 2021), pp. 48-50.

[907] 'Border Violence Monitoring Network' (*BVMN*) <https://www.borderviolence.eu/>.

of boats,[908] effectively disregarding the humanitarian imperative of saving lives at sea. Consequently, the adoption of technologies in external border management is expected to grow even more within the highly technologically militarized border regions, lacking adequate accountability measures and human rights oversight systems.[909] As Molnar argues, the heightened over-reliance on reinforcing border security and surveillance via contemporary technologies of remote control, as highlighted by the new EU Pact on Migration and Asylum with its emphasis on border enforcement and deterrence, also sends a stark message that Europe prioritizes border protection over the safety of human lives.[910]

3. Technologies of Control and Rescue at Sea

Without a doubt the dominant representation of migration and people on the move as problematic to a host community fuels destructive attitudes and allows for stricter security measures to address a supposed threat. The following two examples will map the role of technologies during irregular migrant crossings in the Mediterranean.

The Cutro migrant shipwreck of 26 February 2023 exposes is a vivid illustration of the practice of abandonment at sea and serves as a paradigmatic example of how technologies could have been utilised to advance the human rights and safeguard the lives of migrants but have instead been instrumentalised as a mean to control movement and keep foreigners out. In brief, a Turkish wooden vessel, carrying more than 150 migrants navigated along the Calabria route towards Italy. During its journey, the vessel encountered adverse weather conditions and became in distress as large quantities of water entered the boat. A Frontex aircraft, part of Operation Themis surveilling the area, detected the boat 40 nautical miles from Italy and communicated this information to the Italian law enforcement authorities and those of maritime rescue. Thermal imaging provided information to the authorities that not only the boat was overcrowded but also, that there 'might be people below the deck'.[911] However, no rescue operation was ever launched. Instead, Italy mobilized two patrol boats of Guardia di Finanza (GDF) initiating a police operation to investigate the situation, who had to then return to the port due to bad weather and sea conditions. It is important to stress that the GDF is ill-equipped to conduct a SAR operation; had the Italian coast-guard been deployed

[908] Push-back practices include the forced return of migrants, including applicants for international protection, to the country from where they attempted to cross or have crossed an international border without allowing them to apply for asylum or submit an appeal which may lead to a violation of the principle of non-refoulement. See, European Commission, Migration and Home Affairs 'Glossary', <https://home-affairs.ec.europa.eu/networks/european-migration-network-emn/emn-asylum-and-migration-glossary/glossary/push-back_en#:~:text=Various%20measures%20taken%20by%20states,or%20denied%20of%20any%20individual>.

[909] Molnar E, 'Territorial and Digital Borders and Migrant Vulnerability under a Pandemic Crisis' in Anna Triandafyllidou (ed.), *Migration and Pandemics* (IMISCOE Research Series, 2021), p. 48.

[910] Ibid.; Sunderland J, 'EU's Migration Pact is a Disaster for Migrants and Asylum Seekers' (HRW, 21 December 2023) <https://www.hrw.org/news/2023/12/21/eus-migration-pact-disaster-migrants-and-asylum-seekers?gad_source=1&gclid=CjwKCAjw_e2wBhAEEiwAyFFFo5PQm7SXzqMovjQ9LBFfJR1JanQ-EU2DtRmGspTJqhR3nJIXVmYLORoCmp8QAvD_BwE>.

[911] Nielsen N, 'Crotone shipwreck triggers police vs coastguard blame game' (*EU Observer*, 2 March 2023) <https://euobserver.com/migration/156776>.

though, they would have been able to navigate and undertake a SAR, even under worse weather conditions, as they are professionally equipped to undertake such rescue missions.[912]

While *in casu* there was no distress call from the migrants to alert the Italian authorities of their need of assistance at sea, the use of surveillance technology by Frontex, altered the relevant authorities of a strong likelihood of an emergency that arguably should have been marked as a Search and Rescue event. It appears that the primary cause of this human tragedy stems from Italy's negligent acts vis-à-vis failure to launch a SAR mission within its SAR zone, resulting in fatal consequences. Whilst in the case Frontex submitted that there appeared to be 'no signs of distress', the evidence from the surveillance technology indicated strong elements that the vessel was in distress as it showed a high number of people on board with adverse sea conditions, meaning that the situation at sea was extremely perilous.[913] Importantly, the 1979 International Convention on Maritime Search and Rescue (SAR Convention) provides Article 2.1.9 of the Annex that 'on *receiving information* that a person is in distress at sea in an area within which a Party provides for the overall co-ordination of search and rescue operations, the responsible authorities of that Party shall take urgent steps to provide the most appropriate assistance available'.[914] This is also reflected in Regulation 33 Chapter V of the 1974 International Convention for the Safety of Life at Sea with reference to shipmasters who are in a position to be able to provide assistance 'on receiving information *from any source*' (emphasis added).[915]

Hence the existence of positive information about a vessel in danger signifies a reasonably certain distress situation that reaches the threshold of the application of the duty to render assistance at sea. This is further supported by the international law of the sea framework, which provides that coastal States have authority over distress incidents in their SAR zone. This entails a due diligence obligation, requiring authorities to exercise best efforts to activate available SAR services in that geographical area and employ all adequate measures to save lives.[916]

Another example is the *Nivin* incident of 2018. In this case, a Spanish surveillance aircraft (part of the then EU's anti-smuggling mission Operation *Sophia*) spotted a migrant's boat in the Libya SAR zone and passed this information to both the Italian and Libyan Coast Guards, who then instructed a Panama-flagged merchant vessel that was nearby, the *Nivin*, to take all rescuees back to Libya, in violation of their rights. The incident resulted in an individual complaint currently before the Committee, the *SDG v Italy*.[917] The argument put forth is that the Italian authorities through their

[912] Italian Post News, 'Shipwreck, prosecutor investigates rescued delays' (*Italian Post*, 2 March 2023) <https://www.italianpost.news/shipwreck-prosecutor-investigates-rescued-delays/>.

[913] Papachristodoulou A, 'Shipwreck after Shipwreck: Frontex Emergency Signals and the Integration of AI systems' (Verfassungsblog, 11 March 2024) <https://verfassungsblog.de/shipwreck-after-shipwreck/>.

[914] Emphasis added.

[915] International Convention for the Safety of Life at Sea, 1974, as amended, 1184 UNTS 278 (adopted 1 November 1974, entered into force 25 May 1980).

[916] UN, 'State Responsibility: Second Report on State Responsibility, by Mr. James Crawford, Special Rapporteur', UN Doc. A/CN.4/498 (1999) <https://legal.un.org/ilc/documentation/english/a_cn4_498.pdf>.

[917] 'Communication to the United Nations Human Rights Committee In the Case of SDG against Italy

coordination with and on behalf of the Libyan Coast Guard and Navy (LCGN) of the *Nivin*, had impacted the right to life of the individuals involved, in a direct and reasonably foreseeable manner.

Evidently, the Italian authorities acquired the relevant knowledge about the migrant's boat in distress by virtue of the data transmitted by the said Spanish surveillance aircraft. As the LCGN could not deploy its own vessels to perform the 'rescue' of migrants at that time, the *Nivin* was instructed on their behalf to undertake the task.[918] In what followed, migrants realized that they were taken back to Libya and locked themselves in the hold of the ship, resulting in a standoff in the port of Misrata which lasted ten days. The Libyan security forces then intervened and forcefully removed the captured passengers from the vessel and subjected them to various forms of ill-treatment, including torture. This case illuminates the systematic pattern of EU aerial surveillance strategies that facilitate the privatized pushbacks of migrants to Libya, impede access to asylum and expose migrants to abuse and threats to life.[919] Manifestly, technology has been a great ally in preventing migrants from reaching Europe and accessing protection. It remains yet to be seen what the outcome of the *Nivin* incident will be.

From the above illustrations it can be observed that migration technologies currently used and deployed in the Mediterranean have the effects of the banopticon, whereby international waters are used by States as a 'moat' to keep the unwanted 'others' out by intercepting boats carrying migrants and allowing State governments to invisibly circumvent their international obligations.[920] Therefore, the sea appears to have become a novel form of prison. In this context, Bigo's apparatus of the banopticon helps in comprehending the essence of technologies utilised in *controlling* migration, which exemplifies a process of 'othering'. In fact, the underlying notion of treating migrants with a sense of 'otherness' has evoked a segregated approach towards foreigners, non-nationals, or non-citizens and has resulted in the proliferation of exclusionary bordering practices that are applied from the moment an individual attempts to leave from their country, constituting an absolute denial of the right to asylum. It is important as such to apprehend that the banopticon is rooted in the belief that control will only be for *others*. In this context, as FitzGerald has noted, the goal of remote control practices is to control the *mobility* of individuals while they are outside their intended State' territory destination.[921] The urge to tie and address the unprecedented implications of technologies on the law, and, in particular, on human rights is profound. Hence, this

(Anonymized Version) Submitted for Consideration under the Optional Protocol to the International Covenant on Civil and Political Rights to The United Nations Human Rights Committee' (*GLAN*, 2019) <https://www.academia.edu/41462159/Communication_to_the_United_Nations_Human_Rights_Committee_In_the_case_of_SDG_v_Italy>.

[918] 'Privatized Push-Back of the Nivin' (*Forensic Architecture*, 18 December 2019) <https://forensic-architecture.org/investigation/nivin>.

[919] GLAN, 'Privatised Migrant Abuse by Italy and Libya' <https://www.glanlaw.org/nivincase>.

[920] FitzGerald D, 'Remote control of migration: theorizing territoriality, shared coercion, and deterrence' (2020) 46(1) *Journal of Ethnic and Migration Studies* 4, p. 12.

[921] Ibid., p. 9.

last section has sought to provide a research agenda for scholars, practitioners and judges alike, to build upon.

Conclusion

Migration technologies are profoundly changing the border control processes within the migration control dispositif, reinforcing the framing of cross-border mobility in the context of risk. Despite such technological advancements having the capacity to make an invisible phenomenon visible, the externalization of Europe's border has led to thousands of avoidable deaths, and push- and pullbacks to Libya, constituting an absolute disregard of the *non-refoulement* principle, the right to life, the right to leave and a bar to protection. It is worrisome that even in the aftermath of the shocking death of more than 600 migrants on 14 June 2023, the EU's response has still not been comprehensive and satisfactory.

All these matters are extremely politically and legally sensitive, leading to much confusion. Nonetheless, technology should not be used as a key to side-line ethical and humanitarian imperatives when dealing with the complex nature of migration. Neither should migration movements be seen as a threat amenable to a technological solution. What ensues from this contribution is the necessity for EU policy decisions to adopt a human rights-based approach to the deployment of technologies in external border management, as human rights norms do apply in these circumstances.

Summary

This monograph offers a structured and comprehensive examination of the intersection between technology and public international law, guiding readers through a range of topics and perspectives that highlight the challenges and opportunities presented by the rapid advancements in the digital age. The conference monograph is divided into seven chapters, each focusing on a specific area of public international law. These chapters provide in-depth analysis and insights into the implications of new technologies on the respective aspects of international legal norms and frameworks.

Chapter I, Humanitarian Law, is divided into two parts. Firstly, **Michael J. Pollard** examines the debate over autonomous weapons systems (AWS), particularly armed swarming drones, and the lack of a broadly agreed definition for AWS. His article underlines the potential breach of International Humanitarian Law if swarms are directed to target individuals based on specific characteristics. According to his view, when interpreted in good faith, AWS deployments may be regarded unlawful under Article 51(5)(b) Additional Protocol I to the Geneva Conventions. This is followed by **Triantafyllos Kouloufakos**, who addresses the vulnerability of critical infrastructure to cyberattacks, emphasizing the challenges in safeguarding them under international law. It investigates potential pathways, with an emphasis on the due diligence obligation of no harm and the non-intervention principle. The first section investigates the no-harm principle's relevance beyond international environmental law, proposing adaptations for usage in cyberspace. The second section delves into the rule prohibiting intervention, analyzing the issues of applying coercion and *domaine réservé* to cyberspace and proposing modification to overcome these difficulties.

Chapter II, International Justice, consists of two contributions. In the first, **Mohamed Gomaa** provides an analysis of the impact of digital transformation (DT) and information and communication technology (ICT) on the efficiency of judicial systems worldwide, particularly in response to the challenges posed by the COVID-19 pandemic. The research involves cross-sectional data analysis of 40 countries, considering parameters such as the number of judges, budget, and disposition time. The findings reveal a significant positive correlation between the use of DT/ICT and improved access to justice. In the second contribution, **Marcin Gudajczyk** raises concerns about the growing reliance on digital technologies and the internet, leading to an increase in cybercrime. He argues that the challenges of obtaining electronic evidence stored in other jurisdictions necessitate the introduction of new cross-border judicial cooperation mechanisms, such as direct requests to foreign digital service providers. Special attention is paid to the Regulation of the European Parliament and Council on European Production Orders and European Preservation Orders, adopted in July 2023, presenting its mechanisms for securing digital evidence and addressing potential controversies and threats in terms of international fair trial standards and human rights protection.

In a diversified **Chapter III, Environmental and Space Law,** first contributor, **Lucia Bakošová**, reflects on the need for legal regulation in the era of Industry 4.0, focusing on the specific difficulties brought by artificial intelligence (AI), especially its

possible influence on human rights and accountability. The manuscript examines the evolution of international human rights law, including the recognition of the right to a clean, healthy, and sustainable environment in 2022, and evaluates whether current or proposed international norms regulating AI consider this newly acknowledged right. She is followed by **Juraj Panigaj**, who addresses the intricate relationship between technology and international legal protection of biological diversity. The paper provides insights into the potential contributions, challenges, and risks associated with technology in the context of international environmental law while also putting existing treaty law under scrutiny and considering the adaptability of legal frameworks to rapid technological advancement. The chapter is rounded up by **Charles Ross Bird**, who focuses on the prohibition of national appropriation in outer space, exploring the current legal landscape, including the Artemis Accords. Based on interpretation of Article 2 of the Outer Space Treaty through the Vienna Convention on the Law of Treaties, he arrives to the conclusion that national appropriation only applies to states rather than private actors.

The assorted **Chapter IV, Region-specific Issues,** is divided in three parts. In the first section, **Pavlína Krausová** explores the transformative role of technology in the tax administrations of developing countries amid the global shift towards digital economies. She demonstrates how modern digital tax systems can not only improve revenue collection and compliance but also contribute to equitable taxation and sustainable development and concludes that the integration of tax and technology in terms of revenue collection should be mindful of protecting individual taxpayers' rights, especially in the realm of cyber-security. The second, provided by **Oshokha Caleb Ilegogie,** focuses on the intersection of Artificial Intelligence (AI) and healthcare and potential benefits and issues of implementing such a system in developing countries. He emphasises the need for collaboration among policymakers, healthcare professionals, and technology experts to establish a proper regulation of AI to ensure it contributes to a just promotion of the right to health while addressing potential risks. Finally, **Nikolas Sabján** examines how new technologies and digitalization have affected sanctions law, specifically focusing on EU cyber sanctions as a specific response to digitalization. He provides an analysis of the EU cyber sanctions regime, discusses international legal aspects, particularly immunity law, and reflects critically on recent academic work in the field, concluding with insights into the consequences of digitalization on sanctions law.

Chapter V, Cyber-crimes, also follows a three-part structure. The chapter opens with the contribution of **Robert Łasa**, who examines the difficulties in prosecuting individuals for war crimes committed in cyberspace, focusing on the absence of specific legal rules and effective mechanisms for criminal proceedings. He differentiates between state-affiliated units and private individuals, highlighting the challenge of holding hackers accountable when acting under state supervision during armed conflicts. The duo co-contributors, **Marek Gerle** & **Adam Crhák,** focus on the significance of the Tallinn Manual in shaping discourse on self-defense and protecting critical infrastructure. They explain the Manual's interpretations of UN Charter Article 2(4) and Article 51 through a comparative analysis which also considers relevant state positions and emerging customary norms. In the third part, **Szymon Skalski** provides a critical examination

of the current approaches to combating cybercrime, emphasizing the limitations of traditional paradigms in adapting to the dynamic nature of cyber threats. It highlights the shortcomings of enumerating specific offenses and advocates for a shift towards dynamic adaptable legal structures that can quickly respond to new risks posed by the cyberspace.

The penultimate **Chapter VI, Cyber-security, and Cyber-defense**, explores two currently discussed topics. **Agata Starkowska** introduces the first topic, where she examines the consequences of violations of international norms in cybersecurity on the case study of the ongoing armed conflict in Ukraine. She further evaluates the sanctions imposed on Russia for breaching cyber-security obligations through an analysis of UN Charter provisions and reports from UN working groups. Predicting the future role of cyberattacks in modern warfare and the effectiveness of international law in countering cybercrime, she concludes with insights on Poland's stance and the role of the Cybersec Forum. Secondly, **Michał Byczyński's** part concerns *infodemia*, a phenomenon of quickly spreading false information and deceptive claims that was amplified by the COVID-19 pandemic. Michał elaborates on its impact on human rights and possible strategies for promoting trustworthy information in the public sphere. He further advocates for information hygiene, emphasising the role of international law in combating *infodemia* with potential utility of AI and machine learning in identifying and countering misinformation.

The collective monograph is concluded with **Chapter VII, Human rights**, which consists of three contributions. In the first, **Foto Pappa** addresses the potential societal impact of digital agriculture, highlighting concerns about power asymmetries and inequalities among farmers. She emphasises the necessity of measures such as their involvement in the decision-making to preemptively address risks and proposes examining the human right to science, research, and innovation. **Veronika D'Evereux** follows with an examination of Israel's National Artificial Intelligence plan while outlining the legal challenges associated with AI use in the public sector. She explains the issues with the absence of universally accepted legal rules for AI usage, particularly in addressing human rights concerns related to terrorism and security threats. Finally, **Aphrodite Papachristodoulou** takes an in-depth look at the irregular migration by sea in the Mediterranean and a deadly shipwreck near Pylos, Greece and its human rights implications. She takes a critical stance towards the perceived shift to digital border management, arguing that it exacerbates human rights violations and argues for the adoption of a human rights-based approach to the use of technologies in external border management.

Zusammenfassung

Diese Monographie bietet eine strukturierte und umfassende Untersuchung der Schnittstelle zwischen Technologie und Völkerrecht und führt den Leser durch eine Reihe von Themen und Perspektiven, die die Herausforderungen und Chancen des rasanten Fortschritts im digitalen Zeitalter aufzeigen. Die Konferenzmonographie ist in sieben Kapitel unterteilt, die sich jeweils auf einen bestimmten Bereich des Völkerrechts konzentrieren. Diese Kapitel bieten eingehende Analysen und Einblicke in die Auswirkungen neuer Technologien auf die jeweiligen Aspekte internationaler Rechtsnormen und -rahmen.

Kapitel I, Humanitäres Recht, ist in zwei Teile gegliedert. Zunächst untersucht **Michael J. Pollard** die Debatte über autonome Waffensysteme (AWS), insbesondere bewaffnete Schwarmdrohnen, und das Fehlen einer allgemein anerkannten Definition für AWS. In seinem Artikel unterstreicht er die potenzielle Verletzung des humanitären Völkerrechts, wenn Schwärme auf der Grundlage spezifischer Merkmale auf Personen gerichtet werden. Seiner Ansicht nach können AWS-Einsätze, wenn sie nach Treu und Glauben ausgelegt werden, gemäß Artikel 51 Absatz 5 Buchstabe b des Zusatzprotokolls I zu den Genfer Konventionen als rechtswidrig angesehen werden. Es folgt **Triantafyllos Kouloufakos**, der sich mit der Anfälligkeit kritischer Infrastrukturen für Cyberangriffe befasst und die Herausforderungen beim Schutz dieser Infrastrukturen im Rahmen des Völkerrechts hervorhebt. Es werden mögliche Wege untersucht, wobei der Schwerpunkt auf der Sorgfaltspflicht, keinen Schaden anzurichten, und dem Nichteinmischungsgrundsatz liegt. Der erste Abschnitt untersucht die Relevanz des Grundsatzes der Nichtschädigung über das internationale Umweltrecht hinaus und schlägt Anpassungen für die Anwendung im Cyberspace vor. Der zweite Abschnitt befasst sich mit dem Interventionsverbot, analysiert die Probleme bei der Anwendung von Zwang und *domaine réservé* im Cyberspace und schlägt Änderungen vor, um diese Schwierigkeiten zu überwinden.

Kapitel II, Internationale Justiz, besteht aus zwei Beiträgen. **Mohamed Gomaa zuerst** analysiert die Auswirkungen der digitalen Transformation (DT) und der Informations- und Kommunikationstechnologie (IKT) auf die Effizienz der Justizsysteme weltweit, insbesondere im Hinblick auf die Herausforderungen, die sich durch die COVID-19-Pandemie ergeben. Die Untersuchung umfasst eine Querschnittsdatenanalyse von 40 Ländern unter Berücksichtigung von Parametern wie der Anzahl der Richter, dem Budget und der Verfahrensdauer. Die Ergebnisse zeigen eine signifikante positive Korrelation zwischen dem Einsatz von DT/ICT und einem verbesserten Zugang zur Justiz. Im zweiten Beitrag äußert **Marcin Gudajczyk** seine Besorgnis über die zunehmende Abhängigkeit von digitalen Technologien und dem Internet, die zu einem Anstieg der Internetkriminalität führt. Er argumentiert, dass die Herausforderungen bei der Beschaffung elektronischer Beweismittel, die in anderen Gerichtsbarkeiten gespeichert sind, die Einführung neuer Mechanismen der grenzüberschreitenden justiziellen Zusammenarbeit erfordern, wie z. B. direkte Anfragen an ausländische Anbieter digitaler Dienste. Besonderes Augenmerk wird auf die im Juli

2023 verabschiedete Verordnung des Europäischen Parlaments und des Rates über Europäische Herstellungsanordnungen und Europäische Sicherstellungsanordnungen gelegt, in der die Mechanismen zur Sicherung digitaler Beweismittel vorgestellt und potenzielle Kontroversen und Bedrohungen im Hinblick auf internationale Standards für faire Gerichtsverfahren und den Schutz der Menschenrechte angesprochen werden.

In einem abwechslungsreichen **Kapitel III, Umwelt- und Weltraumrecht,** reflektiert die erste Autorin, **Lucia Bakošová**, über die Notwendigkeit einer rechtlichen Regulierung im Zeitalter der Industrie 4.0 und konzentriert sich dabei auf die besonderen Schwierigkeiten, die die künstliche Intelligenz (KI) mit sich bringt, insbesondere auf ihren möglichen Einfluss auf die Menschenrechte und die Rechenschaftspflicht. Der Beitrag untersucht die Entwicklung der internationalen Menschenrechtsgesetze, einschließlich der Anerkennung des Rechts auf eine saubere, gesunde und nachhaltige Umwelt im Jahr 2022, und bewertet, ob aktuelle oder vorgeschlagene internationale Normen zur Regulierung von KI dieses neu anerkannte Recht berücksichtigen. Anschließend befasst sich **Juraj Panigaj** mit der komplizierten Beziehung zwischen Technologie und internationalem Rechtsschutz der biologischen Vielfalt. Die Analyse gibt Einblicke in die potenziellen Beiträge, Herausforderungen und Risiken, die mit der Technologie im Kontext des internationalen Umweltrechts verbunden sind, während er gleichzeitig das bestehende Vertragsrecht auf den Prüfstand stellt und die Anpassungsfähigkeit der rechtlichen Rahmenbedingungen an den raschen technologischen Fortschritt untersucht. Abgerundet wird das Kapitel durch **Charles Ross Bird**, der sich auf das Verbot der nationalen Aneignung im Weltraum konzentriert und dabei die aktuelle Rechtslage, einschließlich der Artemis-Abkommen, untersucht. Auf der Grundlage der Auslegung von Artikel 2 des Weltraumvertrags durch das Wiener Übereinkommen über das Recht der Verträge kommt er zu dem Schluss, dass die nationale Aneignung nur für Staaten und nicht für private Akteure gilt.

Das gegliederte **Kapitel IV, Regionale Fragen,** ist in drei Teile unterteilt. Im ersten Abschnitt untersucht **Pavlína Krausová** die transformative Rolle der Technologie in den Steuerverwaltungen der Entwicklungsländer vor dem Hintergrund des globalen Wandels hin zu digitalen Volkswirtschaften. Sie zeigt auf, wie moderne digitale Steuersysteme nicht nur die Steuererhebung und die Einhaltung der Vorschriften verbessern, sondern auch zu Steuergerechtigkeit und nachhaltiger Entwicklung beitragen können, und kommt zu dem Schluss, dass bei der Integration von Steuern und Technologie im Hinblick auf die Steuererhebung der Schutz der Rechte des einzelnen Steuerzahlers berücksichtigt werden sollte, insbesondere im Bereich der Cybersicherheit. Der zweite Beitrag von **Oshokha Caleb Ilegogie** befasst sich mit der Schnittstelle zwischen künstlicher Intelligenz (KI) und dem Gesundheitswesen sowie den möglichen Vorteilen und Problemen bei der Einführung eines solchen Systems in Entwicklungsländern. Er betont die Notwendigkeit der Zusammenarbeit zwischen politischen Entscheidungsträgern, Fachleuten des Gesundheitswesens und Technologieexperten, um eine angemessene Regulierung der KI zu erreichen, damit sie zu einer gerechten Förderung des Rechts auf Gesundheit beiträgt und gleichzeitig potenziellen Risiken entgegenwirkt. Schließlich untersucht **Nikolas Sabján**, wie sich neue Technologien und die Digitalisierung auf das Sanktionsrecht ausgewirkt haben,

wobei er sich insbesondere auf die EU-Cybersanktionen als spezifische Reaktion auf die Digitalisierung konzentriert. Er analysiert das EU-Cybersanktionssystem, erörtert völkerrechtliche Aspekte, insbesondere das Immunitätsrecht, und setzt sich kritisch mit neueren wissenschaftlichen Arbeiten auf diesem Gebiet auseinander, um abschließend einen Einblick in die Auswirkungen der Digitalisierung auf das Sanktionsrecht zu geben.

Kapitel V, Cybercrime, folgt ebenfalls einer dreiteiligen Struktur. Das Kapitel beginnt mit dem Beitrag von **Robert Łasa**, der die Schwierigkeiten bei der strafrechtlichen Verfolgung von Einzelpersonen für im Cyberspace begangene Kriegsverbrechen untersucht und sich dabei auf das Fehlen spezifischer rechtlicher Vorschriften und wirksamer Mechanismen für Strafverfahren konzentriert. Er unterscheidet zwischen staatlich organisierten Einheiten und Privatpersonen und hebt die Herausforderung hervor, Hacker zur Rechenschaft zu ziehen, wenn sie während bewaffneter Konflikte unter staatlicher Aufsicht handeln. Die beiden Mitautoren **Marek Gerle** und **Adam Crhák** konzentrieren sich auf die Bedeutung des Tallinn-Handbuchs für die Gestaltung des Diskurses über Selbstverteidigung und den Schutz kritischer Infrastrukturen. Sie erläutern die im Handbuch enthaltenen Auslegungen von Artikel 2 Absatz 4 und Artikel 51 der UN-Charta anhand einer vergleichenden Analyse, die auch einschlägige staatliche Positionen und entstehende Gewohnheitsnormen berücksichtigt. Im dritten Teil bietet **Szymon Skalski** eine kritische Untersuchung der aktuellen Ansätze zur Bekämpfung der Cyberkriminalität und betont die Grenzen traditioneller Paradigmen bei der Anpassung an die dynamische Natur von Cyberbedrohungen. Er hebt die Unzulänglichkeiten der Aufzählung spezifischer Straftatbestände hervor und plädiert für einen Wechsel hin zu dynamischen, anpassungsfähigen Rechtsstrukturen, die schnell auf neue Risiken im Cyberspace reagieren können.

Das vorletzte **Kapitel VI, Cybersicherheit und Cyberverteidigung**, befasst sich mit zwei aktuell diskutierten Themen. **Agata Starkowska** führt in das erste Thema ein, indem sie die Folgen von Verstößen gegen internationale Normen im Bereich der Cybersicherheit am Fallbeispiel des anhaltenden bewaffneten Konflikts in der Ukraine untersucht. Außerdem bewertet sie die Sanktionen, die gegen Russland wegen der Verletzung von Cybersicherheitsverpflichtungen verhängt wurden, anhand einer Analyse der Bestimmungen der UN-Charta und der Berichte von UN-Arbeitsgruppen. Sie prognostiziert die künftige Rolle von Cyberangriffen in der modernen Kriegsführung und die Wirksamkeit des internationalen Rechts bei der Bekämpfung der Cyberkriminalität und schließt mit Einblicken in die Haltung Polens und die Rolle des Cybersec Forums. Der zweite Teil von **Michał Byczyński** befasst sich mit *Infodemie*, einem Phänomen der schnellen Verbreitung falscher Informationen und irreführender Behauptungen, welches durch die COVID-19-Pandemie noch verstärkt wurde. Michał Byczyński geht auf die Auswirkungen auf die Menschenrechte und mögliche Strategien zur Förderung vertrauenswürdiger Informationen im öffentlichen Raum ein. Darüber hinaus plädiert er für Informationshygiene und betont die Rolle des internationalen Rechts bei der Bekämpfung der *Infodemie* mit dem potenziellen Nutzen von KI und maschinellem Lernen bei der Identifizierung und Bekämpfung von Fehlinformationen.

Die kollektive Monografie wird mit **Kapitel VII, Menschenrechte,** abgeschlossen, das aus drei Beiträgen besteht. Im ersten Beitrag befasst sich **Foto Pappa** mit den potenziellen gesellschaftlichen Auswirkungen der digitalen Landwirtschaft und hebt die Bedenken über Machtasymmetrien und Ungleichheiten unter den Landwirten hervor. Sie unterstreicht die Notwendigkeit von Maßnahmen wie die Einbeziehung der Landwirte in die Entscheidungsfindung, um den Risiken vorzubeugen, und schlägt vor, das Menschenrecht auf Wissenschaft, Forschung und Innovation zu prüfen. **Veronika D'Evereux** folgt mit einer Untersuchung des israelischen Nationalen Plans für künstliche Intelligenz und skizziert die rechtlichen Herausforderungen, die mit dem Einsatz von KI im öffentlichen Sektor verbunden sind. Sie erläutert die Probleme, die sich aus dem Fehlen allgemein anerkannter rechtlicher Regeln für den Einsatz von KI ergeben, insbesondere im Hinblick auf Menschenrechtsfragen im Zusammenhang mit Terrorismus und Sicherheitsbedrohungen. Schließlich wirft **Aphrodite Papachristodoulou** einen detaillierten Blick auf die Migrationskrise im Mittelmeer und einen tödlichen Schiffbruch in der Nähe von Pylos, Griechenland, sowie auf die damit verbundenen Auswirkungen auf die Menschenrechte. Sie nimmt eine kritische Haltung gegenüber der wahrgenommenen Verlagerung auf digitales Grenzmanagement ein und argumentiert, dass dies Menschenrechtsverletzungen verschärft. Sie plädiert für die Einführung eines Paradigmas des „intelligenteren Menschenrechtsschutzes", indem sie die extraterritorialen Menschenrechtsverpflichtungen anerkennt, die durch die technologische Überwachung an den Seegrenzen entstehen.

Complete bibliography

Books and book chapters

Abusedra A, Bakar A, Islam MT, 'Use of Cyber Means to Enforce Unilateral Coercive Measures in International Law' in Subedi SP (ed), *Unilateral Sanctions in International Law* (Hart, 2022).

Andriole JA, 'Technology Adoption and Digital Transformation: Rapid Technology Adoption for Digital Transformation' in Andriole JA, Cox T, Khin KM, *The Innovator's Imperative* (Auerbach, 2017).

Barrett PM, *Who Moderates Social Media Giants? A Call to End Outsourcing* (NYU CBHR, 2020).

Bassiouni MC, *International Terrorism and Political Crimes* (Springfield, 1975).

Bassiouni MC, *Introduction to International Criminal Law* (2nd edn, Martinus Nijhoff, 2013).

Beaucillon C, *Research Handbook on Unilateral and Extraterritorial Sanctions* (Elgar, 2021).

Berle I, *Face Recognition Technology: Compulsory Visibility and Its Impact on Privacy and the Confidentiality of Personal Identifiable Images* (Springer, 2020).

Bigo D, 'Detention of Foreigners, States of Exception, and the Social Practices of Control of the Banopticon' in Rajaram and Grundy-Warr (eds), *Borderscapes Hidden Geographies and Politics at Territory's Edge* (1st edn, Univ of Minnesota Press, 2007).

Bradford A, *The Brussels Effect: How the European Union Rules the World* (OUP, 2019).

Brownlie I, *Principles of Public International Law* (6th edn, OUP, 2003).

Brownsword R, Scotford E, Yeung K (eds), *The Oxford Handbook of Law, Regulation and Technology* (OUP, 2017).

Brynjolfsson E, McAfee A, *The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies* (Norton, 2014).

Buchan R, Tsagourias N, *Regulating the Use of Force in International Law Stability and Change* (Elgar, 2021).

Cabrillo F, *The Economics of Courts and Litigation* (Elgar, 2008).

Cassese A, Acquaviva G, Fan M, Whiting A, *International Criminal Law: Cases & Commentary* (OUP, 2013).

Conway W, 'Chapter 30: Can Technology Aid Species Preservation?' in Wilson EO and Peter FM (eds), *Biodiversity* (NAS/SI, 1999).

Cordella A, Contini F, *Digital Technologies for Better Justice: A Toolkit for Action* (*IDB*, 2020).

D'Evereux V, 'Občan a jednotlivec v mezinárodním právu, původ, vývoj a současné otázky spojené s postavením Palestinců' [Citizen and individual in international law, origins, development and contemporary issues related to the position of Palestinians] in Ondřej, J (ed), *Právní postavení jednotlivce v mezinárodním právu – Proměny (vývoj) právního postavení jednotlivce v mezinárodním právu* [Legal status of the individual in international law - Changes (development) of the legal status of the individual in international law] (Faculty of Law, Charles University in Prague, 2020).

Deakin S, Adams Z, *Markesinis and Deakin's Tort Law* (8th edn, OUP, 2019).

Deitel H, Deitel B, *An Introduction to Information Processing* (Elsevier, 1986).

Delerue F, *Cyber Operations and International Law* (CUP, 2020).

Demarais A, *Backfire: How Sanctions Reshape the World against U.S. Interests* (Columbia University Press, 2023).

Detter I, *The Law of War* (CUP, 2000).

Dias T, Coco A, *Cyber Due Diligence in International Law* (Oxford Institute for Ethics Law and Armed Conflict, 2021).

Dijstelbloem H, Meijer A, and Besters M, 'The Migration Machine' in Dijstelbloem H, Meijer A (eds), *Migration and the New Technological Borders of Europe* (Palgrave Macmillan, 2011).

DiMatteo LA, Poncibò C, and Cannarsa M (eds), *The Cambridge Handbook of Artificial Intelligence: Global Perspectives on Law and Ethics* (CUP, 2022).

Dinniss HH, *Cyber Warfare and the Laws of War* (CUP, 2012).

Dupuy PM and Vinuales JE, *International Environmental Law: Second Edition* (CUP, 2018).

Dupuy PM, Le Moli G, and Vinuales JE, 'Customary International Law and the Environment' in Rajamani, L and Peel, J (eds), *The Oxford Handbook of International Environmental Law*, 2nd edn (OUP, 2021).

Duvic-Paoli L-A, *The Prevention Principle in International Environmental Law* (CUP, 2018).

Focarelli C, 'Self-Defence in Cyberspace' in *Research Handbook on International Law and Cyberspace* (Elgar, 2021).

Foucault M, *Discipline and Punish: The Birth of the Prison* (Vintage Books, 1975).

Getz D et al, *Artificial Intelligence, Data Science, and Smart Robotics: First Report* (Haifa, 2018).

Glowka L, Burhenne-Guilmin F et al, *A Guide to the Convention on Biological Diversity* (IUCN, 1994).

Gordon R, Smyth M, and Cornell T, *Sanctions Law* (Hart, 2019).

Hamilton Ortiz, J (ed.), *Industry 4.0: Current Status and Future Trends* (IntechOpen, 2020).

Henderson C, 'The United Nations and the Regulation of Cyber-Security' in *Research Handbook on International Law and Cyberspace* (Elgar, 2021).

Higgins R, *Themes and Theories* (OUP, 2009).

Hillman JE, *The Digital Silk Road: China's Quest to Wire the World and Win the Future* (Harper Business, 2021).

Jankuv J, Lantajová D, Blaškovič K, Buchta T and Arbet D, *Medzinárodná právo verejné, 2. časť* [Public International Law, 2nd part] (Vydavatelství Aleš Čeněk, s. r. o., 2016).

Jennings R and Watts A, *Oppenheim's International Law. Intervention*, 1 (OUP, 2008).

Katsh E and Orna R, *Digital Justice: Technology and the Internet of Disputes* (OUP, 2017).

Kilovaty I, 'The international law of cyber intervention' in Nicholas Tsagourias and Russel Buchan (eds) *Research Handbook on International Law and Cyberspace* (EE, 2nd edition, 2021).

Klučka J, 'General Overview of the Artificial Intelligence and International Law' in Klučka, J, Bakošová, L, and Sisák, Ľ (eds), *Artificial Intelligence from the Perspective of Law and Ethics: Contemporary Issues, Perspectives and Challenges* (Nakladatelství Leges, 2021).

Kulesza J, *Due Diligence in International Law* (Brill, 2016).

Kumar K, Zindani D, and Davim JP, *Industry 4.0: Developments towards the Fourth Industrial Revolution* (Springer, 2019).

Leonard M, *The Age of Unpeace: How Connectivity Causes Conflict* (Penguin, 2022).

Lonardo L, *EU Common Foreign and Security Policy after Lisbon between Law and Geopolitics* (Springer, 2023).

Louka E, *International Environmental Law: Fairness, Effectiveness and World Order* (CUP, 2006).

Madsen LB, *Data-Driven Healthcare: How Analytics and BI Are Transforming the Industry* (Wiley, 2014).

Maljean-Dubois S, 'The No-Harm Principle and the Foundation of International Climate Change Law' in Benoit Mayer and Alexander Zahar (eds) *Debating Climate Law* (CUP, 2021).

Milanovic M, *Extraterritorial Application of Human Rights Treaties* (OUP, 2011).

Molnar E, 'Territorial and Digital Borders and Migrant Vulnerability under a Pandemic Crisis' in Anna Triandafyllidou (ed.), *Migration and Pandemics* (IMISCOE Research Series, 2021).

Oriyano SP and Shimonsky R, 'Mobile Attacks' in Oriyano SP and Shimonsky R, *Client-Side Attacks and Defense* (Elsevier, 2013).

Osop H, Sahama T, 'Data-Driven and Practice-Based Evidence: Design and Development of Efficient and Effective Clinical Decision Support System' in Moon, J.D., *Improving Health Management through Clinical Decision Support Systems* (IGI Global, 2016).

Papastavridis E, 'Rescuing Migrants at Sea and the Law of International Responsibility' in Gammeltoft-Hansen T and Vedsted-Hansen J (eds), *Human Rights and the Dark Side of Globalisation: Transnational Law Enforcement and Migration Control* (T&F, 2016).

Peters A, Krieger H and Kreuzer L 'Due Diligence in the International Legal Order Dissecting the Leitmotif of Current Accountability Debates' Peters A, Krieger H, Kreuzer L (eds), *Due Diligence in the International Legal Order* (OUP, 2020).

Poole DL, Mackworth AK, *Artificial Intelligence: Foundations of Computational Agents* (CUP, 2010).

Quattrocolo S, *Artificial Intelligence, Computational Modelling and Criminal Proceedings: A Framework for A European Legal Discussion* (Springer, 2020).

Rayfuse R, 'Public International Law and the Regulation of Emerging Technologies' in Brownsword, R, Scotford, E, and Yeung, K (eds), *The Oxford Handbook of Law, Regulation and Technology* (OUP, 2017).

Rijpma J, 'Brave New Borders: The EU's Use of New Technologies for the Management of Migration and Asylum' in Cremona (ed.), *New Technologies and EU Law* (OUP, 2017).

Roscini M, *Cyber Operations and the Use of Force in International Law* (OUP, 2014).

Russo R, 'Reflections about the Implications of Platforms and Technology for Taxation and Taxpayers' Rights' in Weber D (ed), *The Implications of Online Platforms and Technology on Taxation* (IBFD, 2023).

Ruys T, 'Immunity, Inviolability and Countermeasures – A Closer Look at Non-UN Targeted Sanctions' in Ruys T, Angelet N, and Ferro L (eds), *The Cambridge Handbook of Immunities and International Law* (CUP, 2019).

Schmitt M, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (CUP, 2017).

Schmitt M, *Tallinn Manual on the International Law Applicable to Cyber Warfare* (CUP, 2013).

Schmitt M, 'The Use of Cyber Force and International Law' in Weller, M. (ed), *The Oxford Handbook of the Use of Force in International Law* (OUP, 2015).

Sheikh MR, Rehman IU, Abbas M and Tariq M, 'Digital Transformation Corruption and Economic Growth Nexus in Asian Countries' (2021) *International Transaction Journal of Engineering, Management, & Applied Sciences & Technologies* 12(6), 12A6N, pp. 1–12.

Steelman DC, *Caseflow Management: The Heart of Court Management in the New Millennium* (NCSC, 2004).

Strážnická V (ed), *Medzinárodná a európska ochrana ľudských práv* [International and European Protection of Human Rights] (Eurokódex, 2013).

Šturma P, Čepelka Č, *Mezinárodní právo veřejné*, 2. vydání [Public International Law, 2nd edition] (C. H. Beck, 2018).

Talbot E, 'Due Diligence in Cyber Activities' in Peters A, Krieger H, Kreuzer L (eds), *Due Diligence in the International Legal Order* (OUP, 2020).

Tessier C, *Robots autonomy: Some technical issues', Autonomy and Artificial Intelligence: A Threat or Savior?* (Springer, 2017).

Tsagourias N & Biggio G, 'Cyber-peacekeeping and international law' in *Research Handbook on International Law and Cyberspace* (Elgar, 2021).

Tsagourias N, 'The legal status of cyberspace: sovereignty redux?' In *Research Handbook on International Law and Cyberspace* (Elgar, 2021).

Uygun Y, *Industry 4.0: Principles, Effects and Challenges* (Nova Sci Publ, 2020).

Wachter R, *The Digital Doctor: Hope, Hype, and Harm at the Dawn of Medicine's Computer Age* (McGraw-Hill Education, 2017).

Worona J, *Cyberspace and International Law – Status Quo and Prospects* (Białystok, 2017).

Zhou J, *Fundamentals of Military Law: A Chinese Perspective* (Springer, 2019).

Journal Articles

Abdelminaam DS, Ismail FH, Taha M, Taha A, Houssein EH, Nabil A. 'CoAID-DEEP: An Optimized Intelligent Framework for Automated Detecting COVID-19 Misleading Information on Twitter.' (2021) 9 *IEEE Access* 27840.

Abhimanyu GJ, 'Rationalising International Law Rules on Self-Defence: The Pin-Prick Doctrine' (2014) XII(2) *Chi.-Kent J. Int'l & Comp. L.* 23.

Acharya A, Estevadeordal A, and Goodman, LW, 'Multipolar or Multiplex? Interaction Capacity, Global Cooperation and World Order' (2023) 99 *International Affairs* 2339.

Agarwal R et al, 'Addressing Algorithmic Bias and the Perpetuation of Health Inequities: An AI Bias Aware Framework' (2023) 12 *Health Policy and Technology* 100702.

Albarello F, Pianura E, Di Stefano F, Cristofaro M, Petrone A, Marchioni L, Palazzolo C, Schininà V, Nicastri E, Petrosillo N, Campioni P, Eskild P, Zumla A, Ippolito G; COVID 19 INMI Study Group '2019-novel Coronavirus severe adult respiratory distress syndrome in two cases in Italy: An uncommon radiological presentation' (2020) 93 *International Journal of Infectious Diseases* 192.

Alegre S, 'Rethinking Freedom of Thought for the 21st Century' (2017) 3 *European Human Rights Law Review* 221.

Ali M, Shifa AB, Shimeles A & Woldeyes F, 'Building Fiscal Capacity in Developing Countries: Evidence on the Role of Information Technology' (2021) 74(3) *National Tax Journal* 591.

Ali S et al, 'Explainable Artificial Intelligence (XAI): What We Know and What Is Left to Attain Trustworthy Artificial Intelligence' (2023) 99 *Information Fusion* 101805.

Alm J, 'Tax Evasion, Technology, and Inequality' (2021) 22(4) *Economics of Governance* 321.

Al-Rakhami MS and Al-Amri AM, 'Lies Kill, Facts Save: Detecting COVID-19 Misinformation in Twitter' (2020) 8 *IEEE Access* 155961.

Amann DM and Sellers M, 'The United States of America and the International Criminal Court' (2002) 50 *The American Journal of Comparative Law* 381.

Amoore M, Marmura S and Salter M, 'Editorial: Smart Borders and Mobilities: Spaces, Zones, Enclosures' (2022) 5(2) *Surveillance & Society* 96.

Bannelier K, 'Rien Que La Lex Lata"? Étude Critique Du Manuel de Tallinn 2.0 Sur Le Droit International Applicable Aux Cyber-Opérations' (2017) 63 *Annuaire français de droit international* 121.

Bannelier-Christakis K, 'Cyber Diligence: A Low-Intensity Due Diligence Principle for Low-Intensity Cyber Operations?' (2015) 14(1) *Baltic Yearbook of International Law* 23.

Baron R, 'A Critique of the International Cybercrime Treaty' (2002) 10 *CommLaw Conspectus* 263.

Baumgartner R et al, 'Fair and Equitable AI in Biomedical Research and Healthcare: Social Science Perspectives' (2023) 144 *Artificial Intelligence in Medicine* 102658.

Bellon M, 'Technology and Tax Compliance Spillovers: Evidence from a VAT E-Invoicing Reform in Peru' (2023) 212 *Journal of Economic Behavior & Organization* 756.

Berberi A et al, 'Enablers, Barriers, and Future Considerations for Living Lab Effectiveness in Environmental and Agricultural Sustainability Transitions: A Review of Studies Evaluating Living Labs' (2023) 1 *Local Environment* 1.

Bertot JC, Estevez E, Janowski T, 'Universal and contextualized public services: Digital public service innovation framework' (2016) 33(2) *Government Information Quarterly* 211.

Besson S, 'Anticipation under the human right to science: concepts, stakes and specificities' (2024) 28(3) *The International Journal of Human Rights* 293.

Bini SA, 'Artificial Intelligence, Machine Learning, Deep Learning, and Cognitive Computing: What Do These Terms Mean and How Will They Impact Health Care?' (2018) 33 *J. Arthroplast* 2358.

Bird R and Zolt E, 'Technology and Taxation in Developing Countries: From Hand to Mouse' (2008) 61 *National Tax Journal* 791.

Boer LJM, 'Restating the Law as It Is: On the Tallinn Manual and the Use of Force in Cyberspace' (2013) 5 *Amsterdam LF* 4.

Bogdanova I and Vásquez Callo-Müller M, 'Unilateral Cyber Sanctions: Between Questioned Legality and Normative Value' (2021) 54 *Vanderbilt J. Transnat'l L* 911.

Bohr A and Memarzadeh K, 'The rise of artificial intelligence in healthcare applications' (2020) 12(3) *Artificial Intelligence in Healthcare* 25.

Bronson K, 'Looking through a Responsible Innovation Lens at Uneven Engagements with Digital Farming' (2019) 90–91(1) *NJAS – Wageningen Journal of Life Sciences* 1.

Bronson K, 'Smart Farming: Including Rights Holders for Responsible Agricultural Innovation' (2018) 8 *Technology Innovation Management Review* 7.

Brunk I, 'Central Bank Immunity, Sanctions, and Sovereign Wealth Funds' (2023) 91 *George Washington Law Review* 1616.

Brunnée J, 'Procedure and Substance in International Environmental Law' (2020) 405 *Hague Academy Collected Courses* 70.

Bublitz C et al, 'Legal Liabilities of BCI-Users: Responsibility Gaps at the Intersection of Mind and Machine?' (2019) 65 *International Journal of Law and Psychiatry* 101399.

Buchan R, 'Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?' (2012) 17 *Journal of Conflict and Security Law* 21.

Buchan R, 'Cyberspace, Non-State Actors and the Obligation to Prevent Transboundary Harm' (2016) 21(3) *Journal of Conflict & Security Law* 429.

Buga I, 'The Impact of Subsequent Customary International Law on Treaties: Pushing the Boundaries of Interpretation' (2022) 69 *Netherlands International Law Review* 241.

Burchardt D, 'Does Digitalization Change International Law Structurally?' (2023) 24 *German Law Journal* 438.

Chachko E, 'Foreign Affairs in Court: Lessons from CJEU Targeted Sanctions Jurisprudence' (2019) 44 *Yale Journal of International Law* 1.

Chen A, Wang C and Zhang X, 'Reflection on the Equitable Attribution of Responsibility for Artificial Intelligence-Assisted Diagnosis and Treatment Decisions' (2023) 3 *Intelligent Medicine* 139.

Chen I, Szolovits P and Ghassemi M, 'Can AI Help Reduce Disparities in General Medical and Mental Health Care?' (2019) 21(2) *The AMA Journal of Ethics* 167.

Chen YY et al, 'Exploring Shodan From the Perspective of Industrial Control Systems' (2020) 8 *IEEE Access* 75359.

Choukri I, 'Remarques Sur Les Manuels de Tallinn (1.0 et 2.0) et Le Droit International Applicable Aux Cyber-Opérations' (2018) 10 *PSEI* 1.

Chuanying L, 'The Digital Silk Road: China's Quest to Wire the World and Win the Future' (2023) 99(3) *International Affairs* 1359.

Claudia CC, Verini SS, de Alteriis G et al, 'Using Drone Swarms as a Countermeasure of Radar Detection' (2023) 20 *Journal of Aerospace Information Systems* 2.

Coco A, Dias T and van Benthem T, 'Illegal: The SolarWinds Hack under International Law' (2022) 33(4) *European Journal of International Law* 1275.

Couzigou I, 'Securing Cyber Space: The Obligation of States to Prevent Harmful International Cyber Operations' (2018) 32 *International Review of Law, Computers & Technology* 37.

Cristani F, 'Economic Cyber-Espionage in the Visegrád Four Countries: A Hungarian Perspective' (2021) 17 *Politics in Central Europe* 697.

Cuan-Baltazar JY, Muñoz-Perez MJ, Robledo-Vega C, Pérez-Zepeda MF and Soto-Vega E, 'Misinformation of COVID-19 on the Internet: Infodemiology Study' (2020) 6(2) *JMIR Public Health Surveill* 18444.

Davenport T and Kalakota R, 'The Potential for Artificial Intelligence in Healthcare' (2019) 6 *Future Healthcare Journal* 94.

De Abreu MJ, 'Acts Is Acts Tautology and Theopolitical Form' (2021) 64 *Social Analysis* 42.

Deng H, 'What can China do to develop International Criminal Law and Justice further from the perspective of the International Criminal Court?' (2016) 5 *Revista Tribuna Internacional* 9.

Deplano R, 'The Artemis Accords: Evolution or Revolution in International Space Law' (2021) 70 *ICLQ* 799.

D'Evereux V, 'K některým otázkám vývoje státního občanství na území dnešního státu Izrael a na palestinském území' [Selected Issues of the Development of Citizenship in the Territory of Today's State of Israel and the Palestinian Territories] (2020) 3 *AUCI* 65.

D'Evereux V, 'K postavení menšin na území státu Izrael v kontextu mezinárodního práva a zákona o národním státě' [The Legal Position of Minorities in the Territory of the State of Israel in the Context of Public International Law and the "Nation State Law"] (2021) 3 *AUCI* 129.

Dong Y, 'The Jus Ad Bellum in Cyberspace: Where Are We Now and What next?' (2019) 17 *NZJPIL* 41.

Donoghue J, 'The Rise of Digital Justice: Courtroom Technology, Public Participation and Access to Justice: The Rise of Digital Justice' (2017) 80 *Modern Law Review* 995.

Downey Jr WG, 'The Law of War and Military Necessity' (1953) 47 *AJIL* 2.

Drukker L, Noble JA and Papageorghiou AT, 'Introduction to artificial intelligence in ultrasound imaging in Obstetrics and Gynecology' (2020) 56 *Ultrasound Obstetr Gynecol* 498.

Ebrahimi HP, Schillo RS and Bronson K, 'Systematic Stakeholder Inclusion in Digital Agriculture: A Framework and Application to Canada' (2021) 13 *Sustainability* 1.

Efrony D and Shany Y, 'A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice' (2018) 112 *American Journal of International Law* 583.

El Bilali H, 'Relation between Innovation and Sustainability in the Agro-Food System' (2018) 30 *Italian Journal of Food Science* 200.

Faúndez A, Mellado-Silva R and Aldunate-Lizana E, 'Use of Artificial Intelligence by Tax Administrations: An Analysis Regarding Taxpayers' Rights in Latin American Countries' (2020) 38 *Computer Law & Security Review* 105441.

Felbermayr G et al, 'The Global Sanctions Data Base' (2020) 129 *European Economic Review* 1.

Finger R, 'Digital Innovations for Sustainable and Resilient Agricultural Systems' (2023) 50 *European Review of Agricultural Economics* 1277.

Finlay L and Payne C, 'The Attribution Problem and Cyber Armed Attacks' (2019) 113 *AJIL Unbound* 202.

FitzGerald D, 'Remote control of migration: theorizing territoriality, shared coercion, and deterrence' (2020) 46(1) *Journal of Ethnic and Migration Studies* 4.

Fleck D, 'Searching for International Rules Applicable to Cyber Warfare – A Critical First Assessment of the New Tallinn Manual' (2013) 18 *J Conflict & Sec L* 331.

Floridi L and Cowls J, 'A Unified Framework of Five Principles for AI in Society' (2019) 1(1) *Harvard Data Science Review* 1.

Floridi L, Cowls J, Beltrametti M et al, 'AI4People — An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations' (2018) 28 *Minds and Machines* 689.

Forney J and Dwiartama A, 'The Project, the Everyday, and Reflexivity in Sociotechnical Agri-Food Assemblages: Proposing a Conceptual Model of Digitalisation' (2023) 40 *Agriculture and Human Values* 441.

Fountain JE, 'The moon, the ghetto and artificial intelligence: Reducing systemic racism in computational algorithms' (2022) 39 *Governmental Information Quarterly* 101645.

Fraser A, '"You Can't Eat Data"?: Moving beyond the Misconfigured Innovations of Smart Farming' (2022) 91 *Journal of Rural Studies* 200.

Gaivoronskaya Y, 'Digitalization risks and threats' (2020) 8 *Advances in Law Studies* 25.

Gardezi M et al, 'In Pursuit of Responsible Innovation for Precision Agriculture Technologies' (2022) 9(2) *Journal of Responsible Innovation* 224.

Gardocki S and Wrona J, 'Russia's use of cyberspace in hybrid conflicts in the light of Russian cyber security policy' (2020) 2(38) *Colloquium* 33.

Genge B and Enăchescu C, 'ShoVAT: Shodan-based Vulnerability Assessment Tool for Internet-facing Services' (2016) 9 *Secur. Commun. Netw.* 2698.

Ghráinne M, 'Left to Die at Sea: State Responsibility for the May 2015 Thai, Indonesian and Malaysian Pushback Operations' (2017) 10 *Irish Yearbook of International Law* 1.

Gorove S, 'Interpreting Article II of the Outer Space Treaty' (1969) 37 *Fordham L. Rev.* 349.

Gregory A and Halff G, 'The Damage Done by Big Data-Driven Public Relations' (2020) 46 *Public Relations Review* 101902.

Gremmen B, Blok V and Bovenkerk B, 'Responsible Innovation for Life: Five Challenges Agriculture Offers for Responsible Innovation in Agriculture and Food, and the Necessity of an Ethics of Innovation' (2019) 32 *Journal of Agricultural and Environmental Ethics* 673.

Gunning D et al, 'XAI—Explainable Artificial Intelligence' (2019) 4(37) *Science Robotics* 7120.

Guo J and Li B, 'The Application of Medical Artificial Intelligence Technology in Rural Areas of Developing Countries' (2018) 2 *Health Equity* 174.

Habersaat KB, Betsch C, Danchin M, Sunstein CR, Böhm R, Falk A, Brewer NT, Omer SB, Scherzer M and Sah S, 'Ten considerations for effectively managing the COVID-19 transition' (2020) 4 *Nature Human Behaviour* 677.

Hackfort S, 'Patterns of Inequalities in Digital Agriculture: A Systematic Literature Review' (2021) 13 *Sustainability* 1.

Hajduk J and Stępniewski T, 'Russia's Hybrid War with Ukraine: Determinants, Instruments, Accomplishments and Challenges' (2016) 2 *Studia Europejskie – Studies in European Affairs* 37.

Hameleers M, van den Meer T and Vliegenhart R, 'Civilized Truths, Hateful Lies? Incivility and Hate Speech in False Information – Evidence from Fact-Checked Statements in the US.' (2021) 25(11) *Information, Communication & Society* 1596.

Hassan B, 'Artificial Intelligence in Social Security: Opportunities and Challenges' (2022) 20(3) *The Journal of Social Policy Studies* 407.

Hathaway O et al, 'The Law of Cyber-Attack' (2012) 100 *California Law Review* 817.

He J et al, 'The Practical Implementation of Artificial Intelligence Technologies in Medicine' (2019) 25 *Nature Medicine* 30.

Henchion MM et al, 'Developing "Smart" Dairy Farming Responsive to Farmers and Consumer-Citizens: A Review' (2022) 12 *Animals* 1.

Holzinger A, Haibe-Kains B, Jurisica I, 'Why Imaging Data Alone Is Not Enough: AI-Based Integration of Imaging, Omics, and Clinical Data' (2019) 46 *European Journal of Nuclear Medicine and Molecular Imaging* 2722.

Hunter B, Hindocha S and Lee RW, 'The role of artificial intelligence in early cancer diagnosis' (2022) 14(6) *Cancers* 1524.

Ingram J and Maye D, 'What Are the Implications of Digitalisation for Agricultural Knowledge?' (2020) 4 *Frontiers in Sustainable Food Systems* 1.

Jackson-Smith D and Veisi H, 'A Typology to Guide Design and Assessment of Participatory Farming Research Projects' (2023) 5 *Socio-Ecological Practice Research* 159.

Jakku E et al. 'Reflecting on Opportunities and Challenges Regarding Implementation of Responsible Digital Agri-Technology Innovation' (2022) 62 *Sociologia Ruralis* 363.

Jamnejad M and Wood M, 'The Principle of Non-Intervention' (2009) 22 *Leiden Journal of International Law* 345.

Jemiluyi OO, 'Tax Revenue Mobilization Effort in Southern African Development Community (SADC) Bloc: Does ICT Matter?' (2023) 11(1) *Cogent Economics & Finance* 1.

Jianjun L, Xuan W and Yaping W, 'Can Government Improve Tax Compliance by Adopting Advanced Information Technology? Evidence from the Golden Tax Project III in China' (2020) 93 *Economic Modelling* 384.

Joshi S et al, 'Modeling Conceptual Framework for Implementing Barriers of AI in Public Healthcare for Improving Operational Excellence: Experiences from Developing Countries' (2022) 14 *Sustainability* 11698.

Kalmady SV et al, 'Towards Artificial Intelligence in Mental Health by Improving Schizophrenia Prediction with Multiple Brain Parcellation Ensemble-Learning' (2019) 5(1) *Schizophrenia* 2.

Karageorgou V, 'The Environmental Integration Principle in EU Law: Normative Content and Function also in Light of New Developments, such as the European Green Deal' (2023) 8(1) *European Papers* 159.

Kastner JK et al, 'An Expert Consultation System for Frontline Health Workers in Primary Eye Care' (1984) 8 *Journal of Medical Systems* 389.

Khan S, Hakak S, Deepa N, Prabadevi B, Dev K, Trelova S, 'Detecting COVID-19-Related Fake News Using Feature Extraction' (2022) 9 *Frontiers in Public Health* 788074.

Kilovaty I, 'Doxfare: Politically Motivated Leaks and the Future of the Norm on Non-Intervention in the Era of Waponized Information' (2018) 9 *Harv. Nat'l Sec. J.* 146.

Kilovaty I, 'The Elephant in the Room: Coercion' (2019) 113 *American Journal of International Law Unbound* 87.

Kim H and Xie B, 'Health Literacy in the eHealth Era: A Systematic Review of the Literature' (2017) 100 *Patient Education and Counseling* 1073.

Kleinpeter E, 'Four Ethical Issues of 'E-Health'' (2017) 38 *IRBM* 245.

Könönen J, 'Legal geographies of irregular migration: An outlook on immigration detention' (2020) 26(5) *Population Space and Place* 2340.

Kukk M, Põder A and Viira A-H, 'The Role of Public Policies in the Digitalisation of the Agri-Food Sector. A Systematic Review' (2022) 94 *NJAS: Impact in Agricultural and Life Sciences* 217.

Kükrer C and Eğmir RT, 'Perception of Tax Office Employees for the Use of Blockchain Technology in Tax Office' (2019) 6(12) *International Journal of Advanced Research* 638.

La Fors K, Custers B and Keymolen E, 'Reassessing Values for Emerging Big Data Technologies: Integrating Design-Based and Application-Based Approaches' (2019) 21 *Ethics and Information Technology* 209.

Lawrence G, 'Global Health Law Governance' (2008) 22 *Emory International Law Review* 35.

Lazarotto B, 'The Impact of Disinformation During the COVID-19 Pandemic and Its Regulation by the EU' (2020) 6 *EU Law Journal* 2.

Leal Filho W et al, 'Deploying Artificial Intelligence for Climate Change Adaptation' (2022) 180 *Technological Forecasting & Social Change* 121662.

Lee RJ, 'Article II of the Outer Space Treaty: Prohibition of State Sovereignty, Private Property Rights, or Both' (2004) 11 *Austl. INT'L L.J.* 128.

Li W et al, 'The Making of Responsible Innovation and Technology: An Overview and Framework' (2023) 6 *Smart Cities* 1996.

Lioutas ED and Charatsari C, 'Innovating Digitally: The New Texture of Practices in Agriculture 4.0' (2022) 62 *Sociologia Ruralis* 250.

Luor T, Wang JF and Lu HP, 'Trends in and Contributions to Tallinn Manual Research: An Assessment of the Literature from 1998 to November 2022' (2023) 27 *Informatica Economica* 45.

Lutterbeck D, 'Airpower and Migration Control' (2023) 28(5) *Geopolitics* 2016.

Lyons J, 'Documenting Violations of International Humanitarian Law from Space: A Critical Review of Geospatial Analysis of Satellite Imagery during Armed Conflicts in Gaza (2009), Georgia (2008), and Sri Lanka (2009)' (2012) 94(886) *International Review of the Red Cross* 739.

Macak K, 'Decoding Article 8 of the International Law Commission's Articles on State Responsibility: Attribution of Cyber Operations by Non-State Actors' (2016) 21(3) *Journal of Conflict and Security Law* 405.

Macak K, 'On the Shelf, but Close at Hand: The Contribution of Non-State Initiatives to International Cyber Law' (2019) 113 *AJIL Unbound* 81.

Macfarlane NBW et al, 'Direct and Indirect Impacts of Synthetic Biology on Biodiversity Conservation' (2022) 25(11) *iScience* 105423.

Małecka A, 'Cyber operations under international law' (2022) 3(47) *Colloquium* 149.

Manheim K and Kaplan L, 'Artificial Intelligence: Risks to Privacy and Democracy' (2019) 21 *Yale JL & Tech* 106.

McCampbell M, Schumann C and Klerkx L, 'Good Intentions in Complex Realities: Challenges for Designing Responsibly in Digital Agriculture in Low-Income Countries' (2022) 62 *Sociologia Ruralis* 279.

McCarthy J, Minsky ML, Rochester N and Shannon CE, 'A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence, August 31, 1955' (2006) 27(4) *AI Magazine* 12.

McDougal M and Feliciano F, 'International Coercion and World Public Order: The General Principles of the Law of War' (1958) 67 *Yale Law Journal* 771.

Mehrabi N et al, 'A Survey on Bias and Fairness in Machine Learning' (2021) 54(6) *ACM Computing Surveys* 1.

Mehrabi Z et al, 'The Global Divide in Data-Driven Farming' (2021) 4 *Nature Sustainability* 154.

Miadzvetskaya Y and Wessel AR, 'The Externalisation of the EU's Cybersecurity Regime: The Cyber Diplomacy Toolbox' (2022) 7 *European Papers* 413.

Milanovic M, 'Revisiting Coercion as an Element of Prohibited Intervention in International Law' (2023) 117(4) *American Journal of International Law* 601.

Mishra A, 'State-Centric Approach to Human Rights: Exploring Human Obligations' (2019) 32 *Rev Quebecoise de Droit Int'l* 49.

Mittelstadt BD et al, 'The Ethics of Algorithms: Mapping the Debate' (2016) 3(2) *Big Data & Society* 1.

Molina N et al, 'Farmers' Participation in Operational Groups to Foster Innovation in the Agricultural Sector: An Italian Case Study' (2021) 13 *Sustainability* 1.

Mooney P, 'What's cooking for climate change-technofixing dinner for 10 billion' (2018) 74(6) *Bulletin of the Atomic Scientists* 390.

Morley J et al, 'The Ethics of AI in Health Care: A Mapping Review' (2020) 260 *Social Science & Medicine* 113172.

Moulin T, 'Reviving the Principle of Non-Intervention in Cyberspace: The Path Forward' (2020) 25(3) *Journal of Conflict & Security Law* 437.

Müller A, 'Anticipation under the human right to science (HRS): sketching the public institutional framework. The example of scientific responses to the appearance of SARS-CoV-2' (2024) 28(3) *The International Journal of Human Rights* 439.

Müller J, Mitesser O, Schaefer HM et al, 'Soundscapes and Deep Learning Enable Tracking Biodiversity Recovery in Tropical Forests' (2023) 14 *Nat Commun* 6191.

Naik N et al, 'Legal and Ethical Consideration in Artificial Intelligence in Healthcare: Who Takes Responsibility?' (2022) 9 *Frontiers in Surgery* 1.

Nedeski N, Sparks T and Hernandez GI, 'The World Is Burning, Urgently And Irreparably: A Plea for Interim Protection against Climatic Change at the ICJ' (2023) 22(2) *The Law & Practice of International Courts and Tribunals* 301.

Nezhmetdinova FT et al, 'Risks of Modern Biotechnologies and Legal Aspects of Their Implementation in Agriculture' (2020) 17 *BIO Web of Conferences* 227.

Obermeyer Z et al, 'Dissecting Racial Bias in an Algorithm Used to Manage the Health of Populations' (2019) 366 *Science* 447.

Okunogbe O and Pouliquen V, 'Technology, Taxation, and Corruption: Evidence from the Introduction of Electronic Tax Filing' (2022) 14(1) *American Economic Journal: Economic Policy* 341.

Okunogbe O and Santoro F, 'The Promise and Limitations of Information Technology for Tax Mobilization' (2023) 38(2) *The World Bank Research Observer* 295.

Onah CK et al, 'Physician Emigration from Nigeria and the Associated Factors: The Implications to Safeguarding the Nigeria Health System' (2022) 20 *Human Resources for Health* 80.

Owoyemi A et al, 'Artificial Intelligence for Healthcare in Africa' (2020) 2 *Frontiers in Digital Health* 1.

Perveen N and Ahmad A, 'Tax Technology, Fairness Perception and Tax Compliance among Individual Taxpayers' (2023) 2(2) *Audit and Accounting Review* 99.

Peters DH et al, 'Poverty and Access to Health Care in Developing Countries' (2008) 1136 *Annals of the New York Academy of Sciences* 161.

Pimm SL, Alibhai S, Bergl R et al, 'Emerging Technologies to Conserve Biodiversity' (2015) 30(11) *Trends Ecol Evol* 685.

Ploug T and Holm S, 'The Right to Refuse Diagnostics and Treatment Planning by Artificial Intelligence' (2019) 23 *Medicine, Health Care and Philosophy* 107.

Poli S and Sommario E, 'The Rationale and the Perils of Failing to Invoke State Responsibility for Cyber-Attacks: The Case of the EU Cyber Sanctions' (2023) 24 *German Law Journal* 522.

Prabu M and Shanmugalakshmi R, 'An Overview of Side Channel Attacks and Its Countermeasures using Elliptic Curve Cryptography' (2010) 2 *IJCSE* 1492.

Racine E, Boehlen W and Sample M, 'Healthcare Uses of Artificial Intelligence: Challenges and Opportunities for Growth' (2019) 32 *Healthcare Management Forum* 272.

Radai Y, 'The Israeli PC Virus' (1989) 8(2) *Computers & Security* 111.

Ramesh A et al, 'Artificial Intelligence in Medicine' (2004) 86 *Annals of The Royal College of Surgeons of England* 334.

Regan Á, 'Exploring the Readiness of Publicly Funded Researchers to Practice Responsible Research and Innovation in Digital Agriculture' (2021) 8 *Journal of Responsible Innovation* 28.

Reisman E, 'Sanitizing Agri-Food Tech: COVID-19 and the Politics of Expectation' (2021) 48 *Journal of Peasant Studies* 910.

Roberts A, Choer Moraes H and Ferguson V, 'Toward a Geoeconomic Order in International Trade and Investment' (2019) 22 *Journal of International Economic Law* 655.

Rosales V, 'Economics of Court Performance: An Empirical Analysis' (2008) *European* 25 *Journal of Law and Economics* 231.

Roscini M, 'World wide warfare: Jus ad bellum and the use of cyber force' (2010) *14 Max Planck YBUNL* 85.

Rose DC and Chilvers J, 'Agriculture 4.0: Broadening Responsible Innovation in an Era of Smart Farming' (2018) 2 *Frontiers in Sustainable Food Systems* 1.

Ruess AK, Müller R and Pfotenhauer SM, 'Opportunity or Responsibility? Tracing Co-Creation in the European Policy Discourse' (2023) 50 *Science and Public Policy* 433.

Ruger JP, 'Toward a Theory of a Right to Health: Capability and Incompletely Theorized Agreements' (2006) 18 (2) *Yale J Law Humanit* 273.

Sandbrook C, Clark D, Toivonen T et al, 'Principles for the socially responsible use of conservation monitoring technology and data' (2021) 3(5) *Conservation Science and Practice* 374.

Schillings J, Bennett R and Rose DC, 'Managing End-User Participation for the Adoption of Digital Livestock Technologies: Expectations, Performance, Relationships, and Support' (2024) 30 (2) *The Journal of Agricultural Education and Extension* 277.

Schmeier S and Gupta J, 'The Principle of No Significant Harm in International Water Law' (2020) 20 *International Environmental Agreements: Politics, Law and Economics* 597.

Schmitt M and Vihul L, 'Sovereignty in Cyberspace: Lex Lata Vel Non?' (2017) 111 *AJIL Unbound* 213.

Schmitt M, '"Virtual" Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law' (2018) 19 *Chicago Journal of International Law* 30.

Schmitt M, 'Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework' (1999) 37 *Colum J Transnat'l L* 885.

Schmitt M, 'Grey Zones in the International Law of Cyberspace' (2017) 42 *Yale Journal of International Law* 1.

Schmitt M, 'In Defense of Due Diligence in Cyberspace' (2015–2016) 125 *The Yale Law Journal Forum* 68.

Schönberger D, 'Artificial intelligence in healthcare: a critical analysis of the legal and ethical implications' (2019) 27(2) *Int. J. Law Info Technol.* 171.

Sharma K, Fiechter M, George T et al. 'Conservation and people: Towards an ethical code of conduct for the use of camera traps in wildlife research' (2020) 1 *Ecol Solut Evidence* 12033.

Simelton E and McCampbell M, 'Do Digital Climate Services for Farmers Encourage Resilient Farming Practices? Pinpointing Gaps through the Responsible Research and Innovation Framework' (2021) 11 *Agriculture* 1.

Sofaer AD, 'The Sixth Annual Waldemar A. Solf Lecture in International Law: Terrorism, the Law, and the National Defense' (1989) 126 *Mil L Rev* 89.

Sousa WG et al, 'How and Where Is Artificial Intelligence in the Public Sector Going? A Literature Review and Research Agenda' (2019) 36 *Government Information Quarterly* 101392.

Sparrow R, 'Killer Robots' (2007) 24(1) *Journal of Applied Philosophy* 62.

Speaker T, O'Donnell S, Wittemyer G et al, 'A Global Community-Sourced Assessment of the State of Conservation Technology' (2022) 36(3) *Conserv Biol* 13871.

Spiezia F, 'International Cooperation and Protection of Victims in Cyberspace: Welcoming Protocol II to the Budapest Convention on Cybercrime' (2022) 23(1) *ERA Forum* 101.

Spijkerboer T, 'Moving Migrants, States, and Rights: Human Rights and Border Deaths' (2013) 7(2) *Law and Ethics of Human Rights* 213.

Staats JL et al, 'Measuring Judicial Performance in Latin America' (2005) 47(4) *Latin American Politics and Society* 77.

Steinke J et al, 'Participatory Design of Digital Innovation in Agricultural Research-for-Development: Insights from Practice' (2022) 195 *Agricultural Systems* 1.

Stilgoe J, Owen R and Macnaghten P, 'Developing a framework for responsible innovation' (2013) 42(9) *Research Policy* 1568.

Stock R and Gardezi M, 'Make Bloom and Let Wither: Biopolitics of Precision Agriculture at the Dawn of Surveillance Capitalism' (2021) 122 *Geoforum* 193.

Stoumpos AI, Kitsios F and Talias MA, 'Digital Transformation in Healthcare: Technology Acceptance and Its Applications' (2023) 20 *International Journal of Environmental Research and Public Health* 3407.

Swanson L, 'The Era of Cyber Warfare: Applying International Humanitarian Law to the 2008 Russian-Georgian Cyber Conflict' (2010) 32 *Loyola of Los Angeles International and Comparative Law Review* 303.

Swire-Thompson B and Lazer D, 'Public Health and Online Misinformation: Challenges and Recommendations' (2020) 41(1) *Annual Review of Public Health* 433.

Taft WH IV, 'Self-Defense and the Oil Platforms Decision' (2004) 29 *Yale J Int'l L* 295.

Takano A, 'Due Diligence Obligations and Transboundary Environmental Harm: Cybersecurity Applications' (2018) 7(4) *Laws* 36.

Tanodomdej P, 'The Tallinn Manuals and the Making of the International Law on Cyber Operations' (2019) 13 *Masaryk U JL & Tech* 67.

Tashtoush Y, Alrababah B, Darwish O, Maabreh M and Alsaedi N, 'A Deep Learning Framework for Detection of COVID-19 Fake News on Social Media Platforms' (2022) 7 *Data* 5.

Tomsky T, 'Citizens of Nowhere: Cosmopolitanisation and Cultures of Securitisation in Dionne Brand's Inventory' (2019) 40(5) *Journal of Intercultural Studies* 564.

Tonekaboni S, Joshi S, McCradden MD and Goldenberg A, 'What clinicians want: Contextualizing explainable machine learning for clinical end use' (2019) 1 *Proceedings of Machine Learning Research* 21.

Tosza S, 'All Evidence is Equal, but Electronic Evidence is More Equal Than Any Other: The Relationship Between the European Investigation Order and the European Production Order' (2020) 11(2) *New Journal of European Criminal Law* 161.

Townsend LC and Noble C, 'Variable Rate Precision Farming and Advisory Services in Scotland: Supporting Responsible Digital Innovation?' (2022) 62 *Sociologia Ruralis* 212.

Tsagourias N, 'The Slow Process of Normativizing Cyberspace' (2019) 113 *AJIL Unbound* 71.

Tzachor A et al, 'Responsible Artificial Intelligence in Agriculture Requires Systemic Understanding of Risks and Externalities' (2022) 4 *Nature Machine Intelligence* 104.

Umar MA and Masud A, 'Why Information Technology is Constrained in Tackling Tax Noncompliance in Developing Countries' (2020) 33(2) *Accounting Research Journal* 307.

Valderrama IJM, 'Legitimacy and the Making of International Tax Law: The Challenges of Multilateralism' (2015) 7(3) *World Tax Journal* 344.

Van Leeuwen C et al, 'Blind Spots in AI' (2021) 23 *ACM SIGKDD Explorations Newsletter* 42.

Varma R, Verma Y, Vijayvargiya P and Churi PP, 'A systematic survey on deep learning and machine learning approaches of fake news detection in the pre-and post-COVID-19 pandemic' (2021) 14 *International Journal of Intelligent Computing and Cybernetics* 617.

Vázquez-Caro J, & Bird, R, 'Benchmarking Tax Administrations in Developing Countries: A Systemic Approach' (2010) 9 *E Journal of Tax Research* 5.

Vereeck L and Mühl M, 'An Economic Theory of Court Delay' (2000) 10(3) *European Journal of Law and Economics* 243.

Vinuesa R, Azizpour H, Leite I et al, 'The role of artificial intelligence in achieving the Sustainable Development Goals' (2020) 11 *Nat Commun* 233.

Visser O, Sippel SR and Thiemann L, 'Imprecision Farming? Examining the (in) Accuracy and Risks of Digital Agriculture' (2021) 86 *Journal of Rural Studies* 623.

Voigt S abd El Bialy N, 'Identifying the determinants of aggregate judicial performance: taxpayers' money well spent?' (2016) 41 *International Review of Law and Economics* 283.

Voigt S, 'Determinants of judicial efficiency: a survey' (2016) 42(2) *European Journal of Law and Economics* 183.

Wachter S, Mittelstadt B and Floridi L, 'Transparent, Explainable, and Accountable AI for Robotics' (2017) 2(6) *Science Robotics* 6080.

Wagner M, 'The Dehumanization of International Law: Legal, Ethical and Political Implications of Autonomous Weapon Systems' (2014) 47 *Vanderbilt Journal of Transnational Law* 1371.

Wakunuma K, Jiya T and Aliyu S, 'Socio-Ethical Implications of Using AI in Accelerating SDG3 in Least Developed Countries' (2020) 4 *Journal of Responsible Technology* 100006.

Walker DI, 'Tax Complexity and Technology' (2022) 97(4) *Indiana Law Journal* 1095.

Waszak PM, Kasprzycka-Waszak W and Kubanek A, 'The Spread of Medical Fake News in Social Media – The Pilot Quantitative Study' (2018) 7(2) *Health Policy and Technology* 115.

Ye L and Yang H, 'From Digital Divide to Social Inclusion: A Tale of Mobile Platform Empowerment in Rural Areas' (2020) 12 *Sustainability* 1.

Yee S, 'Article 38 of the ICJ Statute and Applicable Law: Selected Issues in Recent Cases' (2016) 7 *J Int'l Disp Settlement* 472.

Zerbe Y, 'Cyber-Enabled International State-Sponsored Disinformation Operations and the Role of International Law' (2023) 33 *SRIEL* 49.

Zhao W, 'Cyber Disinformation Operations (CDOs) and a New Paradigm of Non-Intervention' (2020) 27 *U.C. Davis Journal of International Law & Policy* 35.

Zimmermann E, 'Globalization and terrorism' (2011) 27 *European Journal of Political Economy* 152.

Zou J and Schiebinger L, 'AI can be sexist and racist – it's time to make it fair' (2018) 559(7714) *Nature* 324.

Zsófia F, Gyuranecz B and Krausz B, 'The impact of DT on courts' (2022) 7(1) *Cybersecurity and Law* 272.

Case law

ECtHR *Banković v Belgium*, App no 52207/99 (12 December 2001).

ECtHR *Cyprus v Turkey*, App no 25781/94 Judgment (10 May 2001).

ECtHR, *Al-Skeini v. United Kingdom*, Appl. No. 55721/07, Judgment (7 July 2011).

GCC, *Youmans (U.S.) v. United Mexican States*, 4 R.I.A.A. 110, 116 (Gen. Cl. Comm'n 1926).

ICC, *Judgment on the appeal against the decision on the authorisation of an investigation into the situation in the Islamic Republic of Afghanistan*, Judgment [2020] ICC-02/17-138.

ICJ *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro)*, Judgment [2007] ICJ Rep 43.

ICJ, *Case concerning armed activities on the territory of the Congo (DRC v. Uganda)*, Judgment [2005] ICJ Rep 168.

ICJ, *Case Concerning Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America)*, Judgment [1986] ICJ Rep 1986.

ICJ, *Case Concerning Oil Platforms (Islamic Republic of Iran v. United States)*, Judgment [1996] ICJ Rep 2003.

ICJ, *Certain Activities Carried Out by Nicaragua in the Border Area (Costa Rica v. Nicaragua) and Construction of a Road in Costa Rica along the San Juan River (Nicaragua v. Costa Rica)* Merits, Judgment [2015] ICJ Rep 2015.

ICJ, *Corfu Channel (United Kingdom of Great Britain and Northern Ireland v Albania)* Judgment [1949] ICJ Rep 4.

ICJ, *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion [1996] ICJ Rep 1996.

ICJ, *North Sea Continental Self (Federal Republic of Germany/Denmark; Federal Republic of Germany/Netherlands)*, Judgement [1969] ICJ Rep 1969.

ICJ, *Pulp Mills on the River Uruguay (Argentina v Uruguay)*, Judgment [2010] ICJ Rep 2010.

ICJ, *Territorial Dispute (Libyan Arab Jamahiriya/Chad)*, Judgement [1994] ICJ Rep 1994.

ICTY, *Prosecutor v. D. Tadić, Sentencing appeals in the case Dusko Tadic*, CC/P.I.S./465-E (26 January 2000).

ICTY, *Prosecutor v. Kunarac et al., Appeals Chamber Judgement,* IT-96-23 & IT-96-23/1-A (12 June 2002).

ITLOS, *Request for an Advisory Opinion Submitted by the Sub-Regional Fisheries Commission* (*SRFC*), Advisory Opinion [2015] ITLOS Reports 2015.

ITLOS, Seabed Disputes Chamber, *Responsibilities and Obligations of States Sponsoring Persons and Entities with Respect to Activities in the Area*, Advisory Opinion [2011] ITLOS Reports 2011.

PCA, *South China Sea Arbitration, Philippines v. China*, Award of 12 July 2016, PCA Case No 2013-19, ICGJ 495.

PCIJ, *S.S. Lotus (France v. Turkey)* Judgment [1927] PCIJ (Ser. A) No. 10, 18.

Trail Smelter Case (United States of America v. Canada) Judgment (1938, 1941) 3 RIAA 1905 ICJ Rep 29.

International documents

Aarhus Convention on Access to Information, Public Participation in Decision-Making and Access to Justice in Environmental Matters, 25 June 1998, Aarhus, 2161 UNTS 447.

Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, 'Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes' (United Nations, 21 August - 1 September 2023) <https://www.undocs.org/A/AC.291/22>.

Additional Protocol to the American Convention on Human Rights in the Area of Economic, Social, and Cultural Rights: "Protocol of San Salvador", 17 November 1988, San Salvador, El Salvador, OEA/Ser.A/44), Treaty Series no. 69.

Additional Protocol to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts, 8 June 1977, 1125 UNTS 3.

Additional Protocol to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non-International Armed Conflicts, 8 June 1977, 2404 UNTS 609.

Agreement for the Prosecution and Punishment of the Major War Criminals of the European Axis, and Charter of the International Military Tribunal, 8 August 1945, 82 UNTS 251.

Agreement Governing the Activities of States on the Moon and Other Celestial Bodies (1979).

Agreement under the United Nations Convention on the Law of the Sea on the conservation and sustainable use of marine biological diversity in areas beyond national jurisdiction, 19 June 2023. (A/CONF.232/2023/4*), New York (2023).

Arab Charter on Human Rights, League of Arab States (2004).

Asia Initiative, 'Tax Transparency in Asia 2023: Asia Initiative Progress Report', (2023).

Asian Development Bank, *Launching a Digital Tax Administration Transformation: What You Need to Know* (1st ed.), (2022), Asian Development Bank Institute.

Blocking Property of Certain Persons Associated with the International Criminal Court, 11 June 2020, Executive Order 13928.

Cartagena Protocol on Biosafety to the Convention on Biological Diversity (2000), Montreal, 29 January 2000 (Introduction).

CESCR, 'General comment No. 25 on science and economic, social and cultural rights (article 15 (1) (b), (2), (3) and (4) of the International Covenant on Economic, Social and Cultural Rights)' (30 April 2020) UN Doc E/C.12/GC/25.

CESCR, 'Guidelines on Treaty-Specific Documents to be Submitted by States Parties under Articles 16 And 17 of the International Covenant on Economic, Social and Cultural Rights (2009)' UN Doc E/C.12/2008/2.

Convention (IV) Respecting the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land, (1907), 36 Stat. 2277.

Convention on Biological Diversity, June 5, 1982, reprinted in 31 ILM 822 (1992).

Convention on Wetlands of International Importance (known as Ramsar Convention), Feb. 2, 1971, reprinted in 996 UNTS 245.

Council of Europe – Committee on Artificial Intelligence, Consolidated working draft of the Framework Convention on Artificial Intelligence, Hu-man Rights, Democracy and the Rule of Law, 7 July 2023, CAI(2023)18.

Council of Europe – Parliamentary Assembly, Anchoring the right to a healthy environment: need for enhanced action by the Council of Europe, Resolution 2396, (2021).

Council of Europe Commissioner for Human rights, 'Unboxing Artificial Intelligence: 10 Steps to protect Human Rights' (2019).

Council of Europe, 'Assessing the implementation of the Budapest Convention' <https://www.coe.int/en/web/cybercrime/assessments>.

Council of Europe, 'Convention on Cybercrime' (Budapest, 23 September 2001) <https://rm.coe.int/1680081561>.

Council of Europe, 'United Around Our Values' (Reykjavík Declaration), 16 – 17 May 2023.

Council of the European Union, 'Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts', General approach, Brussels, (2022).

Decision adopted by the Conference of the Parties to the Convention on Biological Diversity (CBD/COP/DEC/15/3).

Declaration of the United Nations Conference on the Human Environment. Report of the United Nations Conference on the Human Environment, (June 16, 1972) UN Doc. A/CONF.48/14/Rev. 1.

Documents of the United Nations Conference on International Organization, San Francisco, 1945.

Draft decision submitted by the President: Kunming-Montreal Global biodiversity framework (CBD/COP/15/L.25).

European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14, 4 November 1950, ETS 5.

Geneva Conventions Act 1957, 31 July 1957, UK Public General Acts 1957 c. 52.

Human Rights Committee, 'General Comment No. 34, Article 19: Freedoms of opinion and expression', UN Doc. CCPR/C/GC/34, (2011).

Human Rights Committee, 'General Comment No. 36 on Article 6 of the International Covenant on Civil and Political Rights, on the Right to Life', Adopted by the

Committee at its 124th session (8 October to 2 November 2018). UN Doc. CCPR/C/GC/36, (2018).

Human Rights Council, 'Promotion and Protection of All Human Rights, Civil, Political, Economic, Social and Cultural Rights, Including the Right to Development', A/HRC/47/L.22, (2021).

Human Rights Council, 'Report of the Special Rapporteur on Freedom of Opinion and Expression, OSCE Representative on Freedom of the Media, Special Rapporteur on Freedom of Expression of the Inter-American Commission on Human Rights, and the Special Rapporteur on Freedom of Expression and Access to Information of the African Commission on Human and Peoples' Rights, Joint Declaration on Freedom of Expression and "Fake News", Disinformation, and Propaganda', (2017).

Human Rights Council, 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression', Irene Khan Disinformation and Freedom of Opinion and Expression. UN Doc. A/HRC/47/25, (2021).

Human Rights Council, 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression', UN Doc. A/HRC/38/35, (2018).

Human Rights Council, 'Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression', UN Doc. A/HRC/44/49, (2020).

Human Security in Theory and Practice, United Nations Office for the Coordination of Humanitarian Affairs, (2009).

ICRC position on autonomous weapon systems (*ICRC*, 12 May 2021) <https://www.icrc.org/en/document/icrc-position-autonomous-weapon-systems> accessed 14 December 2023.

ILA, Sadowsky, M. e. c. *White Paper 12 on Taxation: Taxing the Future* (International Law Association (2023).

ILA, 'Study Group on Due Diligence in International Law', First Report, (2014).

ILA, 'Study Group on Due Diligence in International Law', Second Report, (2016).

ILC, 'Draft Articles on Prevention of Transboundary Harm from Hazardous Activities', ILC Yearbook 2001/II(2).

ILC, 'Draft Articles on Jurisdictional Immunities of States and Their Property, with commentaries 1991' (1991).

ILC, 'Draft Articles on Responsibility of States for Internationally Wrongful Acts' UN doc A/56/10, (2001).

ILC, 'Report of the International Law Commission on the Work of its Seventieth Session'.

ILC, 'Survey of State practice relevant to international liability for injurious consequences arising out of acts not prohibited by international law, prepared by the Secretariat', UN Doc A/CN.4/384, (1984).

International Convention for the Safety of Life at Sea, 1974, as amended, 1184 UNTS 278 (adopted 1 November 1974, entered into force 25 May 1980).

International Convention on Maritime Search and Rescue, 1979, with annexes, 1405 UNTS 97 (adopted 27 April 1979, entered into force 22 June 1985).

International Covenant on Economic, Social and Cultural Rights (adopted 16 December 1966, entered into force 3 January 1976) 993 UNTS 3.

International Criminal Court Act 2001, 13 June 2001, UK Public General Acts 2001 c. 17.

International Organisation for Standardization's (SIO) JTC 1/SC 42 Technical committee, (2022).

ITU, 'Constitution and Convention of the International Telecommunication Union (with annexes and optional protocol)', (adopted on 22 December 1992, entered into force 1 July 1994), 1825 UNTS 31251.

OECD, '10 Years of Capacity Building. 2022 Global Forum Capacity Building Report' (2022), <https://www.oecd.org/tax/transparency/documents/2022-Global-Forum-Capacity-Building-Report.pdf >.

OECD, 2023 Progress Report on Tax Co-operation for the 21st Century. *OECD Report for the G7 Finance Ministers and Central Bank Governors* (2023).

OECD, *Automatic Exchange Portal. Common Reporting Standard*. <https://www.oecd.org/tax/automatic-exchange/common-reporting-standard/>.

OECD, *Exchange of Information*. <https://www.oecd.org/ctp/exchange-of-tax-information/>.

OECD, *Forum on Tax Administration* <https://www.oecd.org/tax/forum-on-tax-administration/>.

OECD, 'Guidelines for the Security of Information Systems' (1992).

OECD, 'Guidelines for the Security of Information Systems and Networks' (2002).

OECD, 'Judicial performance and its determinants: a cross-country perspective, A GOING FOR GROWTH REPORT No. 05' (2013).

OECD, 'Policy Framework on Digital Security' (2022).

OECD, 'Principles on Artificial Intelligence', OECD/LEGAL/0449, (2019).

OECD, 'Recommendation of the Council on Artificial Intelligence' (2019).

OECD, 'Supporting the Digitalisation of Developing Country Tax Administrations' (2021).

OHCHR, Türk V, ' Addressing climate and digital challenges: International Geneva', (2023).

Organization of African Unity, 'African Charter on Human and Peoples' Rights ("Banjul Charter")', 27 June 1981, CAB/LEG/67/3 rev. 5, 21 I.L.M. 58 (1982).

Pilloud C, Depruex J, Sandoz Y et al, 'Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949' ICRC, (1987).

Protocol on Prohibitions or Restrictions on the Use of Mines, Booby-Traps and Other Devices, 3 May 1996, 2048 UNTS 93.

Report of the Ad Hoc Technical Expert Group on Synthetic Biology (CBD/SYNBIO/AHTEG/2019/1/3). Montreal, Canada, (4-7 June 2019).

Single Convention on Narcotic Drugs of 1961, the Vienna Convention on Psychotropic Substances of 1971, and the UN Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances of 1988, (1988).

Statute of the International Criminal Court, 17 July 1998, 2187 UNTS 90.

The Artemis Accords Principles for Cooperation in the Civil Exploration and Use of the Moon, Mars, Comets, and Asteroids for Peaceful Purposes (2020).

Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies (1967).

UN Human Rights Council, Report of the Special Rapporteur on the issue of human rights obligations relating to the enjoyment of a safe, clean, healthy and sustainable environment, A/HRC/37/59, (2018).

UN Human Rights Council, Right to a healthy environment: good practices: Report of the Special Rapporteur on the issue of human rights obligations relating to the enjoyment of a safe, clean, healthy and sustainable environment, A/HRC/43/53, (2019).

UN Human Rights Council, The human right to a clean, healthy and sustainable environment, A/HRC/RES/48/13, (2021).

UN Human Rights Office of the High Commissioner, UN Environment Programme, UN Development Programme, What is the Right to Healthy Environment? (2023).

UN Office of the High Commissioner for Human Rights, Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework, New York, and Geneva, (2011).

UN Secretary-General's High-level Panel on Digital Cooperation, The Age of Digital Interdependence, 2019.

UN Statistics Division, Methodology. Standard Country or Area Codes for Statistical Use (M49).

UN, A United Nations system-wide strategic approach and road map for supporting capacity development on artificial intelligence, (2019).

UN, Charter of the United Nations, (1945), 1 UNTS 16

UN, Department of Economic and Social Affairs Population Division, *World Population Prospects 2019, vol II. Nigeria: Demographic Profiles*.

UN, Our Common Agenda Policy Brief 5: A Global Digital Compact – an Open, Free and Secure Digital Future for All, (2023).

UN, Our Common Agenda: Report of the Secretary-General, United Nations, New York, (2021).

UN, 'State Responsibility: Second Report on State Responsibility, by Mr. James Crawford, Special Rapporteur', UN Doc. A/CN.4/498 (1999).

UN, Statute of the International Court of Justice, (1946).

UN, The Sustainable Development Goals Report (2018).

UN, UN Secretary-General launches AI Advisory Body on risks, opportunities, and international governance of artificial intelligence, Press release, (2023).

UNESCO, 'Disinfodemic: Deciphering Covid-19 Disinformation' (2020).

UNESCO, 'Recommendation on the Ethics of Artificial Intelligence' (2021).

UNGA, 'Declaration on Principles of International Law concerning Friendly Relations and Cooperation among States in accordance with the Charter of the United Nations', UN Doc. A/RES/2625(XXV), (1970).

UNGA, 'Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security', UN Doc. A/68/98, (2013).

UNGA, 'Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security', UN Doc. A/70/174, (2015).

UNGA, 'International Covenant on Civil and Political Rights', United Nations, Treaty Series, vol. 999, (1966).

UNGA, 'Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security', UN Doc A/70/17, (2015).

UNGA, 'Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc A/68/98, (2013).

UNGA, 'Report of the Secretary General on Agriculture technology for sustainable development: leaving no one behind', UN Doc A/76/227, (2021).

UNGA, Report of the Special Rapporteur on the issue of human rights obligations relating to the enjoyment of a safe, clean, healthy and sustainable environment, David R. Boyd: The human right to a clean, healthy and sustainable environment: a catalyst for accelerated action to achieve the Sustainable Development Goals, A/77/284, (2022).

UNGA, Res 2131 (XX), 'Declaration on the Inadmissibility of Intervention and Interference in the Internal Affairs of States' UN Doc. A/RES/36/103, (1981).

UNGA, Res 2625 (XXV), Declaration on Principles of International Law Concerning Friendly Relations and Co-operation among States in Accordance with the Charter of the United Nations, (1970) (Friendly Relations Declaration).

UNGA, Res A/C.1/78/L.56, (2023).

UNGA, 'Roadmap for digital cooperation: implementation of the recommendations of the High-level Panel on Digital Cooperation: Report of the Secretary General', A/74/821, (2020).

UNGA, 'Transforming our world: the 2030 Agenda for Sustainable Development', A/RES/70/1, (2015).

UNGA, 'United Nations Convention on Jurisdictional Immunities of States and Their Property', A/RES/59/38, (2004).

UNGA, 'United states of America: Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States submitted by participating governmental experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security established pursuant to General Assembly resolution 73/266', (2021).

UNGA, 'International Covenant on Economic, Social and Cultural Rights', United Nations, Treaty Series, vol. 993 (1966).

UNHCR, 'UNHCR data visualisation on Mediterranean crossings charts rising death toll and tragedy at sea' (2022).

United Nations Convention on the Law of the Sea (adopted 10 December 1982, entered into force 16 November 1994) 1833 UNTS 397 (UNCLOS).

United Nations Inter-Agency Working Group on Artificial Intelligence, Principles for the Ethical Use of Artificial Intelligence in the United Nations System, (2022).

UNODA, 'Costa Rica's Position on the Application of International Law in Cyberspace' (2023).

UNODA, 'Estonia: Official compendium of voluntary national contributions', A/76/136, (2021).

UNODA, 'Norway, Official compendium of voluntary national contributions' A/76/136 (2021).

UNSC, Res. 827 'Statue of the International Criminal Tribunal for the Former Yugoslavia', annex, UN Doc. S/RES/827, (1993).

Vienna Convention on the Law of Treaties (1969) UNTS vol. 1155.

World Bank, 'The Human Capital Index 2020 update: human capital in the time of COVID-19', (2020).

World Health Organization, 'Health workforce: medical doctors'.

World Health Organization, 'Infodemic', (2022).

World Health Organization, 'WHO policy brief: COVID-19 infodemic management', (2022) <https://iris.who.int/bitstream/handle/10665/362668/WHO-2019-nCoV-Policy-Brief-Infodemic-2022.1-eng.pdf?sequence=1>.

World Health Organization, 'World health statistics 2023: Monitoring health for the SDGs, Sustainable Development Goals,' (2023) <https://cdn.who.int/media/docs/default-source/gho-documents/world-health-statistic-reports/2023/world-health-statistics-2023_20230519_.pdf>.

EU documents

Artificial Intelligence Act, EU, P9_TA (2024)0138, 13 March 2024.

Council of European Union, Council Decision (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member State.

Council of European Union, Council Regulation (CFSP) 2019/796 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States.

Council of the European Union, Council Decision (CFSP) 2013/233/ of 22 May 2013 on the European Union Integrated Border Management Assistance Mission in Libya (EUBAM Libya) [2013] OJ L138/15.

Council of the European Union, Council Decision (CFSP) 2020/472 of 31 March 2020 on a European Union Military Operation in the Mediterranean (EUNAVFOR MED IRINI).

Council of the European Union, Cyber-attacks: Council extends sanctions regime until 18 May 2025, Press release.

Council of the European Union, EU sanctions against Russia, Press release <https://www.consilium.europa.eu/en/policies/sanctions/restrictive-measures-against-russia-over-ukraine/>.

Council of the European Union, Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts – General approach, Brussels, 25 November 2022, 14954/22 <https://data.consilium.europa.eu/doc/document/ST-14954-2022-INIT/en/pdf>.

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union [2016] OJ L194/1.

Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union [2022] OJ L333/80.

European Commission, Proposal for a Directive of the European Parliament and of the Council on Liability for Defective Products, repealing Council Directive 85/374/EEC.

European Commission, Proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive AILD) COM (2022).

European Commission, Proposal for a Regulation of the European Parliament and of the Council on Artificial Intelligence (Artificial Intelligence Act), Brussels, 21 April 2021, 2021/0106(COD).

European Commission, 'Document 52021PC0206: Proposal for a Regulation of the European Parliament and of The Council laying down harmonized rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts', 2021/206, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206>.

European Commission, Proposal for a Regulation of the European parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, Brussels. 2021, online, Article 3.

European Law Institute (ELI). ELI Draft of a Revised Product Liability Directive (2022).

European Parliament – Committee on the Environment, Public Health and Food Safety, Opinion of the Committee on the Environment, Public Health and Food Safety for the Committee on the Internal Market and Consumer Protection and for the Committee on Civil Liberties, Justice and Home Affairs on the proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts COM(2021)0206 – C9-0146/2021 – 2021/0106(COD), 22 April 2022.

European Parliament, 'Resolution on the need for EU action on search and rescue in the Mediterranean' (13 July 2023) 2023/2787 (RSP).

European Parliament, Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts COM(2021)0206 – C9-0146/2021 – 2021/0106(COD), <https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_EN.pdf>.

European Union Agency for Fundamental Rights, 'Getting the Future Right. Artificial Intelligence and Fundamental Rights', Report, Luxembourg: Publication office of the European Union, 2020.

European Union, Ethics Guidelines for Trustworthy AI, Independent High-Level Expert Group on Artificial Intelligence Set Up by the European Commission, Brussels, 8 April 2019, <https://op.europa.eu/en/publication-detail/-/publication/d3988569-0434-11ea-8c1f-01aa75ed71a1>.

Market D-G for I and PwC, 'The Scale and Impact of Industrial Espionage and Theft of Trade Secrets through Cyber' (*Publications Office of the EU*, 2018).

Records of the procedure, 2018/0108(COD), COM(2018) 225 final (legislative works).

Regulation (EU) 1052/2013 of the European Parliament and of the Council of 22 October 2013 establishing the European Border Surveillance System (EUROSUR) L 295/11, 6 November 2013.

Regulation (EU) 2019/881, OJ L 151, European Parliament and Council, 17 April 2019.

Regulation (EU) 2023/1543, OJ L 191/118, European Parliament and Council, 12 July 2023.

National legislation

Act on Promotion of Business Activities Related to the Exploration and Development of Space Resources Act No. 83, Japan (2021).

Bill C-27 HC Bill. Canada (2022).

California Legislative Information Bill (Version 04/19/23) AB-331 (2023).

Commercial Space Launch Competitiveness Act, United States (2015).

Connecticut Senate Bill 1103 (2023).

Criminal Code of The Russian Federation No. 63-Fz of 13 June 1996, Russian Federation (1966).

Criminal Law of the People's Republic of China, PRC (1997).

Data Protection Act, Nigeria (2023).

Data Protection Regulation, Nigeria (2019).

International Criminal Court Act c. 17, UK (2001).

Federal Law On the Regulation of the Space Sector (No.12), UAE (2019).

Loi du 20 juillet 2017 sur l'exploration et l'utilisation des ressources de l'espace, Luxembourg (2017).

Military Commissions Act 2006 (c 5) USPL 109-366 (2006).

Notification by the Ministry of Foreign Affairs of the Slovak Republic No. 34/1996 Coll. (1996).

Other sources

'1 Year Anniversary of the Tallinn Manual 2.0 on the International Law applicable to Cyber Operations' (*Dutch Ministry of Defense*, 2018).

'101 Best Israel Big Data Startups & Companies' (*Data Magazine*).

'About Leitmotif 2023' (*CyberSec*).

Addis Tax Initiative, 'The Digital Transformation of Tax Administrations' (*ati*, 19 July 2023).

'AI gun detection helps law enforcement identify active shooter situations' (*Wral News*, 6 October 2023).

'AI has made the Israel Hamas misinformation epidemic much, much worse' (*Rolling Stone*, 2023).

Alberts EC, 'Seventy-plus nations sign historic high seas treaty, paving way for ratification' (*Mongabay*, 22 September 2023).

Albus V, 'Fast-Tracking Law Enforcement at the Expense of Fundamental Rights' (*Verfassungsbolg*, 15 June 2023).

Allen JR and Hussain A, 'On Hyper War' (*Fortuna's Corner,* 2018).

Amnesty International, 'Global: A critical opportunity to ban killer robots – while we still can' (*AI*, 2 November 2021).

Andersen E, 'Measuring the Justice Gap' (*World Justice Project*, 2019).

Antebi L, 'Artificial Intelligence and National Security in Israel.' Memorandum No. 207 (*INSS Tel Aviv University*, 2021).

'Artificial Intelligence (AI) and the government data revolution' (*INDA*, 19 July 2022).

Baggili I (ed), *Digital Forensics and Cyber Crime: Second International ICST Conference, ICDF2C 2010*, Abu Dhabi, United Arab Emirates, October 4–6, 2010, Revised Selected Papers (Springer Berlin Heidelberg 2011).

Baker P, Pistone P, & Turina A, 'The IBFD Yearbook on Taxpayers' Rights 2022' (*IBFD*, 15 May 2023).

Balcewicz J, 'UN GGE – Prawo międzynarodowe w cyberprzestrzeni' (*NASK*, 15 January 2020).

Barela S, 'Cross-border cyber ops to erode legitimacy: An act of coercion' (*Just Security*, 12 January 2017).

BBC World News, 'Gaza Strip in maps: Life in Gaza under siege' (*BBC News*, 8 November 2023).

Bendiek A and Schulze M, 'Attribution: A Major Challenge for EU Cyber Sanctions' (*Stiftung Wissenschaft und Politik (SWP)*).

Berthélémy C, 'e-Evidence compromise blows a hole in fundamental rights safeguards' (*EDRi*, 7 February 2023).

Bertuzzi L, 'e-Evidence: controversy continues in trilogue discussions' (*Euractiv*, 26 May 2021).

Binder C, 'How the EU politicises research and development in border security' (*King's College London*, 21 June 2022).

Boeing, 'Loyal Wingman: Uncrewed but not alone' (*Boeing*, 23 November 2023).

'Border Violence Monitoring Network' (*BVMN*) <https://www.borderviolence.eu/>.

Boyd I, 'How hypersonic missiles work and the unique threats they pose – an aerospace engineer explains' (*The Conversation*, 15 April 2022).

'British soldier admits war crime' (*BBC News*, 30 October 2023).

'Brno University Hospital ransomware attack' (2020) <https://cyberlaw.ccdcoe.org/wiki/Brno_University_Hospital_ransomware_attack_(2020)>.

Buolamwini J, 'Artificial intelligence has a problem with gender and racial bias. Here's how to solve it' (*MIT Media Lab, n.d.*) <https://tinyurl.com/d5546r6p>.

Campaign to Stop Killer Robots, 'Stop Killer Robots' <https://www.stopkillerrobots.org/>.

'Communication to the United Nations Human Rights Committee In the Case of SDG against Italy (Anonymized Version) Submitted for Consideration under the Optional Protocol to the International Covenant on Civil and Political Rights to The United Nations Human Rights Committee' (*GLAN*, 2019).

Cosbey A, & Burgiel S, 'The Cartagena Protocol on Biosafety: An Analysis of Results' (*International Institute for Sustainable Development*, 2000).

'Croatian Prime Minister: Tallinn Manual is an Icebreaker' (*NATO Cooperative Cyber Defence Centre of Excellence visit*, 27 January 2015).

Cueva E, Ee G, Iyer A, Pereira A, Roseman A, & Martinez D, 'Detecting Fake News on Twitter Using Machine Learning Models', Paper presented at the (2020) *IEEE MIT Undergraduate Research Technology Conference (URTC).*

'Cyber and International Law in the 21st Century' (*Gov.uk*, 23 May 2018).

'Cyberatak na Ukrainie. Celem hakerów było czyszczenie danych' (*Wydarzenia*, 23 February 2022).

Daemmrich B, 'Russia Compares Trump's Space Mining Order to Colonialism' (*The Moscow Times*, 7 April 2020).

Davis E, 'First-ever 'State of Conservation Technology' Report Identifies Top 3 Emerging Technologies to Advance Conservation' (*WWF*, 15 December 2021).

'DOD Dictionary of Military and Associated Terms' (*U.S. Department of Defense*, November 2021).

'Droit international appliqué aux opérations dans le cyberespace' (*France, Ministére des Armées*) <https://www.defense.gouv.fr/sites/default/files/ministere-armees/Droit%20international%20appliqu%C3%A9%20aux%20op%C3%A9rations%20dans%20le%20cyberespace.pdf>.

'ECCC to be present at the CYBERSEC Forum & Expo 2023, 21-22 June in Katowice' (*ECCC*, 13 June 2023).

Elkins D, 'Federal Policymakers: Chasing The Runaway AI Train' (*Mondaq*, 16 October 2023).

ENISA, 'Threat Landscape 2022' (*European Union Agency for Cybersecurity*, 2022).

'Environmental Risk Assessment of the Products of Biotechnology' (*Australian Government, Department of Agriculture, Water and the Environment*) <https://www.awe.gov.au/environment/protection/biotechnology>.

European Border and Coast Guard Agency, 'Artificial Intelligence-Based Capabilities for the European Border and Coast Guard Final Report' (*Frontex*, 2021).

'European Commission for the Efficiency of Justice (CEPEJ) CEPEJ Studies' (*Council of Europe portal*) <https://www.coe.int/en/web/cepej>.

'European judicial systems Efficiency and quality of justice CEPEJ STUDIES No. 24' (*Council of Europe portal*) <https://rm.coe.int/european-judicial-systems-efficiency-and-quality-of-justice-cepej-stud/1680788229>.

European Union, Council of Europe and Eurojust, 'International conference on Judicial Cooperation in Cybercrime Matters' (*EU*, 7-8 March 2018).

Ferryman K, Pitcan M, 'Fairness in precision medicine' (*Data & Society*, February 2018).

Finn C, 'Global loss of biodiversity is significantly more alarming than previously suspected' (*Queen's University Belfast*, 23 May 2023).

Foreign, Commonwealth & Development Office, 'Application of international law to states' conduct in cyberspace: UK statement' (*Foreign, Commonwealth & Development Office*, 3 June 2021).

Forrester N, 'A brief history of cyber-threats — from 2000 to 2020' (*Security Brief*, 12 January 2021).

Foust J, 'NASA offers to buy lunar samples to set space resources precedent' (*SpaceNews*, 10 September 2020).

Fox-Sowell S, 'New York lost $775M in cyberattacks on critical infrastructure in 2022, report says' (*Statescoop*, 10 October 2023).

Global Partnership on AI Report, 'Climate Change AI and Centre for AI & Climate, Climate Change and AI: Recommendations for Government' (*GPAI*, November 2021).

Gonfalonieri A, 'A Beginner's Guide to Brain-Computer Interface and Convolutional Neural Networks' (*Medium,* 2018).

Greenfield P, Benato M, 'Animal populations experience average decline of almost 70% since 1970, report reveals' (*The Guardian*, 13 October 2021).

Greenfield P, 'The biodiversity crisis in numbers – a visual guide' (*The Guardian*, 1 December 2022).

GSMA, 'Paying Taxes Through Mobile Money: Initial Insights into P2G and B2G Payments' (*GSMA*, 4 December 2014).

Guerrero S, 'How biotech aids biodiversity' (*Alliance for science*, 17 February 2022).

Hacker P, 'The European AI liability directives – Critique of a half-hearted approach and lessons for the future' (*Cornell University*, 25 November 2022).

Hambling D, 'Israel used world's first AI-guided combat drone swarm in Gaza attacks' (*New Scientist*, 30 June 2021).

Hambling D, 'What are Armed Swarms and Why Does Everyone Suddenly Want one?' (*Forbes*, 1 March 2021).

Hawksworth J, 'AI and Robots Could Create Many Jobs as They Displace' (*World Economic Forum*, 2018).

Hoffman F, 'On Not-So-New Warfare: Political Warfare vs Hybrid Threats' (*War on the Rocks*, 28 July 2014).

Horlacher A and Hess T, (2016). What Does a Chief Digital Officer Do? Managerial Tasks and Roles of a New C-Level Position in the Context of Digital Transformation. In *2016 49th Hawaii International Conference on System Sciences (HICSS)*, Koloa, HI, USA.

'How could AI perpetuate racism, sexism and other biases in society' (*NPR*) <https://tinyurl.com/2p8xa23x>.

Human Rights Watch, 'EU: Frontex Complicit in Abuse in Libya' (*Human Rights Watch*, 12 December 2022).

Human Rights Watch, 'Pressure Point: The ICC's Impact on National Justice' (*HRW*, 3 May 2018).

Chapman A, 'The Foundations of a Human Right to Healthcare: Human Rights and Bioethics in Dialogue, Health and Human Rights' (*HHR*, 9 June 2015).

Chiarelli A, 'Clickjacking Attacks and How to Prevent Them' (Auth0 Blog, 2020) <https://auth0.com/blog/preventing-clickjacking-attacks/>.

Chui M et al, 'Notes From the AI Frontier: Applying AI for Social Good' (*McKinsey Global Institute*, December 2018).

Idika N, & Mathur A, 'A survey of malware detection techniques' (*Purdue University*, 2007) <https://www.researchgate.net/publication/229008321_A_survey_of_malware_detection_techniques>.

'In apparent world first, IDF deployed drone swarms in Gaza fighting' (*The Times of Israel*, 10 July 2021).

'Iran, Victim of Cyber warfare' (*ICRC Casebook*) <https://casebook.icrc.org/case-study/iran-victim-cyber-warfare>.

'Iraq Historic Allegations Team (IHAT)' (*Gov.UK*) <https://www.gov.uk/government/groups/iraq-historic-allegations-team-ihat>.

'Is Israel about to become a leader in quantum computing?' (*Israel21c*, 29 December 2022).

'Israel Defence Force Strategy Document' (*Harvard Kennedy School Belfer Centre for Science and International Affairs*, 2015) <https://tinyurl.com/j3d63npb>.

'Israel is in the front line of cloud computing era' (*Economic and Commercial Mission Consulate General of Israel in Hong Kong*, 2022) <https://tinyurl.com/mryufbw8>.

'Israel IT government encourages 5G cellular Innovation' (*ITA*, 21 March 2023).

'Israel wants a massive supercomputer – no matter the costs' (*Haaretz*, 8 August 2021).

'Israeli scientists study secrets of human brain to bring AI to next level' (*The Jerusalem Post*, 23 April 2020).

Italian Post News, 'Shipwreck, prosecutor investigates rescued delays' (*Italian Post*, 2 March 2023).

'IUCN and AI2 to provide AI technology at no cost to fast-track implementation of newly signed UN High Seas Treaty' (*IUCN*, 21 September 2023).

Jamasmie C, 'Russia slams Trump's order to spur mining on the moon' (*Mining. com*, 9 April 2020).

Judson J, 'US Army awards Boeing, General Atomics contract to develop powerful laser weapon' (*Defence News*, 3 November 2021).

Kanan D, 'Use of digital technologies in judicial reform and access to justice cooperation' (*HiiL*, 2021).

Kapogianni V, 'The Reverberations of the Rise of Fencing Border Regimes: Pushbacks, Detention and Surveillance Technologies' (*International Law Blog*, 21 November 2022).

Kerner SM, 'Colonial Pipeline hack explained: Everything you need to know' (*TechTarget*, 26 April 2022).

KfW Development Bank, 'Information Technology in Tax Administration in Developing Countries' (*KfW*, 2015).

Kitkowska A, Karegar F, & Wästlund E, 'Share or Protect: Understanding the Interplay of Trust, Privacy Concerns, and Data Sharing Purposes in Health and Well-Being Apps' (2023) *CHItaly 2023: 15th Biannual Conference of the Italian SIGCHI Chapter*.

Ku J, 'Tentative Observations on China's Views on International Law and Cyber Warfare' (*Lawfare*, August 26th, 2017).

Lebleu T, 'Technologies to protect biodiversity' (*Solarimpulse Foundation*, 18 April 2019).

Lennon JT, Locey KJ, 'Earth may be home to one trillion species' (*ScienceDaily*, 2 May 2016).

'Letter to the parliament on the international legal order in cyberspace' (*Government of the Netherlands*, July 2019).

'Mandatory e-Invoicing in Rwanda: Electronic Invoicing System (EIS)' (*Edicom,* 22 March 2023).

'Manila Principles on Intermediary Liability' <https://manilaprinciples.org/principles.html>.

Manning C, 'Artificial Intelligence Definitions' (*Stanford University Human-Centered Artificial Intelligence*, 2020).

Marsh S, 'Neurotechnology, Elon Musk and the Goal of Human Enhancement' (*The Guardian*, 1 January 2018).

Maruf R, 'The surprising reason you can't find cream cheese anywhere' (*CNN Business*, 18 December 2021).

Mazibrada A, 'Is there a Right to be Protected from the Adverse Effects of Scientific Progress and its Applications?' (*EJIL: Talk!*, 29 November 2022).

Meltzer J, Tielemans A, 'The European Union AI Act: Next steps and issues for building international cooperation' (*Global Economy and Development at Brookings*, 1 June 2022).

'Memorandum of understanding on cooperation in the fields of development, the fight against illegal immigration, human trafficking and fuel smuggling and on reinforcing the security of borders between the State of Libya and the Italian Republic' (*EU Migration Law Blog*, 2017).

Meridor D, & Eladi R, 'Israel's National Security Doctrine: The Report of the Committee on the Formulation of the National Security Doctrine (Meridor Committee). Ten years later.' (*INSS*, February 2019).

Miadzvetskaya Y, 'Cyber sanctions: towards a European Union cyber intelligence service?' (*College of Europe Policy Brief*, 2021).

Mizokami K, 'The Army's New Drone Killer Can Fry Whole Swarms in Midair' (*Popular mechanics,* 7 November 2023).

Moskva News Agency, 'Russia Plans Long-Term Base on the Moon-Space Agency' *Times* (*Moscow Times*, 6 November 2018).

'National statistics: Why do people come to the UK? To work' (*Gov.UK*, 2022).

Nexon DH, 'Against Great Power Competition' (*Foreign Affairs*, 26 June 2023).

Nguyen A, 'The G7's Fear of Economic Coercion through Weaponised Interdependence – Geopolitical Competition Cloaked in International Law?' (*EJIL*, 22 June 2023).

Nielsen N, 'Crotone shipwreck triggers police vs coastguard blame game' (*EU Observer*, 2 March 2023).

Niemann A and Schmidthäussler N, 'The Logic of EU Policy-Making on (Irregular) Migration: Securitisation or Risk' (*Mainz Papers on International and European Politics*, 2012).

Ning YB, 'How US Evades Responsibility for War Crimes in Afghanistan' (*Global Times*, 27 September 2021).

Norton-Taylor R, 'Britain's spy agencies: the only watchdog is the workforce; The law cannot keep up with technology Parliamentary scrutiny is still far too weak GCHQ employee sacked' (*The Gaudian*, 12 March 2015).

Nowak J, 'Drone Surveillance Operations in the Mediterranean: The Central Role of the Portuguese Economy and State in EU Border Control' (*Border Criminologies*, 26 February 2019).

'Od początku roku SBU zneutralizowała prawie 4 tys. cyberataków na władze i infrastrukturę krytyczną Ukrainy' (*Security Service of Ukraine*, 3 October 2023).

Okunogbe O, 'Becoming Legible to the State: The Role of Identification and Collection Capacity in Taxation (English)' (*World Bank Group*, 2021).

'On the Application of International Law in Cyberspace, Position paper' (*The Federal Government of Germany*, March 2021).

Palczewski S, 'Ataki na Ukraine. SBU podało dane za ten rok' (*CyberDefence 24*, 4 October 2023).

Pawlak P and Biersteker TJ, 'Guardian of the Galaxy. Eu Cyber Sanctions and Norms in Cyberspace' (*Graduate Institute of International and Development Studies*, October 2019).

Peters J, 'Watch DARPA Test Out a Swarm of Drones' (*The Verge*, 9 August 2019).

Piccinini E et al, *Transforming Industrial Business: The Impact of Digital Transformation on Automotive Organizations* (2015).

Press G, '12 Big Data Definitions: What's Yours?' (*Forbes*, 3 September 2014).

'Press release: £2.5-million injection for drone swarms' (*Gov.uk*, 28 March 2019).

'Privatized Push-Back of the Nivin' (*Forensic Architecture*, 18 December 2019).

Raytheon, 'Phalanx Weapon System' (*Raytheon*) <https://tinyurl.com/2mj53kb4>.

Reed J, 'High-impact attacks on critical infrastructure climb 140%' (*Security Intelligence*, 26 June 2023).

Relander B, 'Investing in Green Technology' (*Investopedia*, 31 July 2022).

Ritchie H, 'How many species are there?' (*Our World in Data*, 30 November 2022).

Ruane J and Ramasamy S, 'Global investments in agricultural research: Where are we and where are we going?' (*FAO*, 2023).

Saengphaibul V, 'A Brief History of The Evolution of Malware' (*Fortiguard Labs Threat Research*, 2022).

Sameer Patil, 'Assessing the Efficacy of the West's Autonomous Cyber-Sanctions Regime and Its Relevance for India: EU Cyber Direct' (*Horizon*) <https://eucyberdirect.eu/atlas/sources/assessing-the-efficacy-of-the-west-s-autonomous-cyber-sanctions-regime-and-its-relevance-for-india>.

Santoro M, 'A Regulatory Tsunami is Coming to Silicon Valley: Tech Companies Must Adopt Responsible Innovation or Risk Losing Their Competitive Edge' (*Cambridge Core Blog*, 9 June 2023).

Shakeri F and Human Rights at Sea, 'Crossing the Mediterranean Sea: Searched for but not rescued' (December 2021).

Sheehan M, 'Lloyd's of London launches space insurance policy' *Reinsurance News* (4 December 2019).

Sheer S, 'The State of Artificial Intelligence Israel' (*Innovation Center Denmark*, 2019).

Siddiqui Z, 'Hackers hit aid groups responding to Israel and Gaza crisis' (*Reuters*, 13 October 2023).

'Six Russian GRU officers charged in connection with worldwide deployment of destructive malware and other disruptive actions in cyberspace' (*United States District Court Western District of Pennsylvania*, 19 October 2020).

'Social media platforms swamped with fake news on Israeli Hamas war' (*Al Jazeera*, 10 October 2023).

Soesanto S, 'After a Year of Silence, Are EU Cyber Sanctions Dead?' (*Default*, 26 October 2021).

Sonnenfeldt M, 'It took 30 years for climate tech investments to pay off. Now they're best placed to survive the VC winter' (*FORTUNE*, 26 July 2023).

Starks T, 'What we've learned from a year of Russian cyberattacks in Ukraine' (*Washington Post*, 16 February 2023).

Tangley L, 'How Many Species Exists' (*The National Wildlife Federation*, 1 December 1998).

Tasioulas J, 'The role of the arts and humanities in thinking about artificial intelligence (AI)' (*Ada Lovelace Institute*, 14 June 2021).

Taube F, 'Wojna w Ukrainie. Szczególna rola cyberataków' (*DW*, 1 March 2022).

'The Artemis Plan, NASA's Lunar Exploration Program Overview' (September 2020).

'The European Commission and Tunisia – a stronger partnership' (*European Comission*, 27 April 2023).

'The Gaza Metro: The mysterious subterranean tunnel network used by Hamas' (*CNN*, 28 October 2023).

'The Iraq Historic Allegations Team (IHAT) Quarterly Update' *(The Iraq Historic Allegations Team*, 20 July 2017).

'The Italian position paper on 'International Law and Cyberspace'' (*Italy*, November 2021).

'The terrorists wore our uniforms. IDF soldiers recount the liberation of Israeli communities' (*i24News*, 11 October 2023).

Tsagourias N, 'Electoral cyber interference, self-determination and the principle of non-intervention' (EJIL: *Talk!*, 6 August 2019).

Uenuma F, '20 Years Later, the Y2K Bug Seems Like a Joke—Because Those Behind the Scenes Took It Seriously' (*Time*, 30 December 2019).

Uenuma F, '20 Years Later, the Y2K Bug Seems Like a Joke—Because Those Behind the Scenes Took It Seriously' (*Time*, 30 December 2019).

UN News, 'UN and Red Cross call for restrictions on autonomous weapon systems to protect humanity' (*UN News*, 5 October 2023).

United Nations, 'First Committee Approves New Resolution on Lethal Autonomous Weapons, as Speaker Warns "An Algorithm Must Not Be in Full Control of Decisions Involving Killing"' (*United Nations Press*, 1 November 2023).

Verclytte S, 'Les pré-requis du tribunal numérique' (*Secrétaire général du ministère de la Justice français*, 3 April 2018).

Vosyliūtė L, 'Is saving lives at sea still a priority for the EU' (*Heinrich Böll Stiftung*, 19 April 2018).

Wareham M, 'Killer Robots' (*Human Rights Watch*) <https://www.hrw.org/topic/arms/killer-robots>.

'Warsaw Declaration II' (*Council of Europe*, 2005).

Wedenig S and Nelson JW, 'The Moon Agreement: Hanging by a Thread?' (*McGill Institute of Air and Space Law*, 26 January 2023).

'Who is making sure that AI machines aren't racist' (*The New York Times*, 15 March 2021).

'Why is biodiversity important?' (*The Royal Society*) <https://royalsociety.org/topics-policy/projects/biodiversity/why-is-biodiversity-important/>.

Willmer G, 'Robotic bees and roots offer hope of healthier environment and sufficient food' (*Horizon*, 24 February 2023).

Wrzostek M, 'Dyrektywa NIS, czyli pierwsze europejskie prawo w zakresie cyber-bezpieczeństwa' (*NASK*, 6 July 2016).

Yost S, 'Brave New World: Everything Gets Smarter When 5G and AI Combine' (*Electronic Design*, 11 February 2019).

ELECTRONIC PUBLICATION CREATED BY
rww & SCIENCE & NEW MEDIA
eBOOK PASSAU • BERLIN • PRAGUE

Charles University, Faculty of Law
nám. Curieových 901/7 • 116 40 Praha 1
Czech Republic
https://www.prf.cuni.cz

rw&w
SCIENCE & NEW MEDIA
PASSAU • BERLIN • PRAHA

International Publishing Project
of SüdOst Service GmbH
Waldkirchen, Germany
and Eva Rozkotová Publishers
Beroun, Czechia

ISBN 978-80-87488-55-3
(electronic)